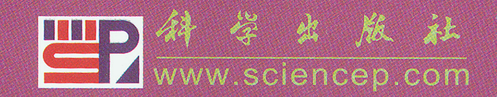
数学名著译丛

代数学II

〔荷〕B.L. 范德瓦尔登 著
曹锡华 曾肯成 郝钢新 译
万哲先 校



数学名著译丛

代 数 学 II

〔荷〕 B. L. 范德瓦尔登 著
曹锡华 曾肯成 郝钢新 译
万哲先 校

科 学 出 版 社
北 京

图字: 01-2009-2859 号

内 容 简 介

全书共分两卷, 涉及的面很广, 可以说概括了 1920–1940 年代数学的主要成就, 也包括了1940年以后代数学的新进展, 是代数学的经典著作之一. 本书是第二卷. 这一卷可分成 3 个独立的章节组: 第 12 至 14 章讨论线性代数、代数和表示论; 第 15 至 17 章是理想理论; 第 18 至 20 章讨论赋值域、代数函数及拓扑代数.

图书在版编目(CIP)数据

代数学. II/(荷)范德瓦尔登(Van der Waerden, B. L.)著; 曹锡华等译. —北京: 科学出版社, 2009
(数学名著译丛)
ISBN 978-7-03-024563-2
I. 代… II. ① 范… ② 曹… III. 高等代数 IV. O15
中国版本图书馆 CIP 数据核字(2008) 第 072339 号

责任编辑: 赵彦超 / 责任校对: 陈玉凤
责任印制: 钱玉芬 / 封面设计: 陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com

中国科学院印刷厂印刷
科学出版社发行 各地新华书店经销
*
2009 年 5 月第 一 版 开本: B5(720 × 1000)
2009 年 5 月第一次印刷 印张: 19
印数: 1—3 000 字数: 362 000

定价: 56.00 元
(如有印装质量问题, 我社负责调换〈环伟〉)

出 版 说 明

范德瓦尔登的《代数学》是现代数学的一部奠基之作, 这部书不仅对提高数学家的学识修养有很大意义, 对现代数学如扑拓学、泛函分析等以及一些其他科学领域也有重要影响.

我社分别于 1963 年和 1976 年出版了该书的中译本上册 (第五版, 丁石孙, 曾肯成, 郝钢新译, 万哲先校) 和下册 (第四版, 曹锡华, 曾肯成, 郝钢新译, 万哲先校). 2003 年, Springer 出版了该书上册 (第七版) 和下册 (第五版). 在丁石孙先生的支持下, 我社委托陈志杰、赵春来两位教授对原中译本进行审校, 修改了一些现在已不常用的名词术语, 如亏数; 纠正了英文版和原中译本中的部分疏漏和错误; 原书第 I 和 II 卷的 “全书综览图” 不同, 这次也按第 II 卷综览图作了统一处理, 等等. 根据 Springer 出版的英译版本补充翻译了部分章节，如第 4 章、第 7.7 节、第 12.7 节、第 19.9 节以及第 20.10–20.14 节.

同时, 我们也积极进行寻找原译者的工作, 但是遗憾的是, 我们只与丁石孙和郝钢新先生及曹锡华先生的夫人陈希伦女士取得了联系, 并得到了他们的大力支持和热情帮助, 请其他译者见到本书后与我们联系.

在此谨向所有译者和审校者表示诚挚的谢意!

中译本再版序言

本书的第七版 (德文版) 于 1966 年由 Springer-Verlag 出版, 1970 年被译成英文出版. 第七版在内容安排上有较大的改动, 还增添了少量内容. 科学出版社的同志认为应当重新翻译本书, 这个想法是好的. 现在的中译本是陈志杰教授在德文第四版的中译本的基础上, 依据 2003 年由 Springer-Verlag 出版的英文平装本整理、翻译而成, 赵春来教授作了校对.

丁石孙

2008 年 12 月

中译本序言

代数学是数学的一个重要的基础的分支, 历史悠久. 我国古代在代数学方面有光辉的成就. 一百多年来, 尤其是 20 世纪以来, 随着数学的发展以及应用的需要, 代数学的研究对象以及研究方法发生了巨大的变革. 一系列的新的代数领域被建立起来, 大大地扩充了代数学的研究范围, 形成了所谓近世代数学. 它与以代数方程的根的计算与分布为研究中心的古典代数学有所不同, 它是以研究数字、文字和更一般元素的代数运算的规律及各种代数结构 —— 群、环、代数、域、格等的性质为其中心问题的. 由于代数运算贯穿在任何数学理论和应用问题里, 也由于代数结构及其中元素的一般性, 近世代数学的研究在数学中是具有基本性的. 它的方法和结果渗透到那些与它相接近的各个不同的数学分支中, 成为一些有着新面貌和新内容的数学领域 —— 代数数论、代数几何、拓扑代数、Lie 群和 Lie 代数、代数拓扑、泛函分析等. 这样, 近世代数学就对于全部现代数学的发展有着显著的影响, 并且对于一些其他的科学领域 (如理论物理学、计算机原理等) 也有较直接的应用。

历史上, 近世代数学可以说是从 19 世纪之初发生的, Galois 应用群的概念对于高次代数方程是否可以用根式来解的问题进行了研究并给出彻底的解答, 他可以说是近世代数学的创始者. 从那时起, 近世代数学由萌芽而成长而发达. 大概由 19 世纪的末叶开始, 群以及紧相联系着的不变量的概念, 在几何上、在分析上以及在理论物理上, 都产生了重大的影响. 深刻研究群以及其他相关的概念, 如环、理想、线性空间、代数等, 应用于代数学各个部分, 这就形成近世代数学更进一步的演进, 完成了以前独立发展着的三个主要方面 —— 代数数论、线性代数及代数、群论的综合. 对于这一步统一的工作, 近代德国代数学派起了主要的作用. 由 Dedekind 及 Hilbert 于 19 世纪末叶的工作开始, Steinitz 于 1911 年发表的论文对于代数学抽象化工作贡献很大, 其后自 1920 年左右起以 Noether 和 Artin 及她和他的学生们为中心, 近世代数学的发展极为灿烂.

Van der Waerden 根据 Noether 和 Artin 的讲稿写成《近世代数学》(*Moderne Algebra*), 综合近世代数学各方面工作于一书. 全书分上、下两册, 第一版于 1930—1931 年分别出版. 自出版后, 这本书对于近世代数学的传播和发展起了巨大的推动作用. 到 1959—1960 年, 上、下两册已分别出到第五版和第四版. 时至今日, 这本书仍然是在近世代数学方面进行学习和开展科学研究的一部好书.

当然, 近世代数学是不断向前发展的. 20 世纪 30 年代, 当时所谓近世代数学的一些基本内容已经逐渐成为每个近代数学工作者必备的理论知识, 所以本书从

50 年代第四版起就去掉“近世”两字而改名为《代数学》, 同时做了较大的增补和改写, 但仍保持着原来的基本内容和风格. 至于 Jacobson 的《抽象代数学讲义》和 Bourbaki 的《代数学》等书, 则出版较后而风格和内容亦有异.

本书的第二版曾有武汉大学故教授萧君绛先生译本, 流传不广, 文字亦较艰涩. 华罗庚先生于 1938—1939 年在昆明西南联合大学讲授近世代数课程时, 曾以本书上册为参考编写讲义, 变动较大而非全文照译. 1961 年 9 月国内代数学工作者于北京颐和园举行座谈会时, 皆认为此书新版有迅速译出之必要. 经过一年, 由曹锡华、万哲先、丁石孙、曾肯成、郝钢新诸同志集体合作译出第一、二卷. 今后当能对代数学的教学及科学研究起较大的推动作用. 更希望国内代数学工作者在教学和科学研究实践中有自著的书籍写成出版.

段学复

1962 年 10 月 11 日

于北京大学数学力学系

第五版前言

非常感谢 P. Roquette 提供给我代数微分 udz 的留数定理的漂亮证明, 使得"代数函数"一章有了一个满意的结尾.

在"拓扑代数"一章里, 依照 Bourbaki, 利用滤网实现群、环和域的完备化, 而不是使用第二可数性公理.

有许多重要应用的"线性代数"一章现在移到了卷首,"拓扑代数"放到了最后. 本书现在可以分成三个独立的章节组:

第 12~14 章: 线性代数, 代数, 表示论;

第 15~17 章: 理想论;

第 18~20 章: 赋值域, 代数函数, 拓扑代数.

综览图更清楚地说明了内容间的联系.

B. L. 范德瓦尔登

苏黎世, 1967 年 3 月

第四版前言

第二卷的开始增添了新的两章. 一章叙述单变量的代数函数, 直到得出任意常数域上的 Riemann-Roch 定理; 另一章讨论拓扑代数, 主要考虑拓扑群、环与体的完备化, 以及局部有界和局部紧致体的理论. Fischer 博士审慎地阅读了这两章的手稿, 作者对他所提出的许多有益的意见表示感谢.

“一般理想论”一章中收进了 Krull 关于素理想的形式幂及素理想链的重要定理, 从而作了扩充.

在“代数整量”一章中把整闭环中理想论与赋值论的关系表达得更清楚了. 在“线性代数”一章中增加了关于反对称双线性型的新的一节 (12.8 节).

“代数”一章中例子增多了. 按照 Jacobson 的方式不附加有限条件发展了根的理论. 更强调了 Noether 关于模的直和与直交的观念. 将 Jacobson 的方法与 Noether 的方法相互结合起来, 可以大大地简化几个主要定理的证明.

作者力图通过精简使得本书的篇幅不超出一个可容许的限度, 因此删去了消去法论一章. 关于齐次方程的结式的存在定理, 过去是通过消去法来证明的, 现在在 16.5 节中作为 Hilbert 零点定理的一个推论而出现.

作者感谢 W. Bandler, J. J. Burckhardt 博士, H. Gross 和 H. Keller 博士诸位先生, 他们在校订手稿及阅读校样中给予宝贵的帮助.

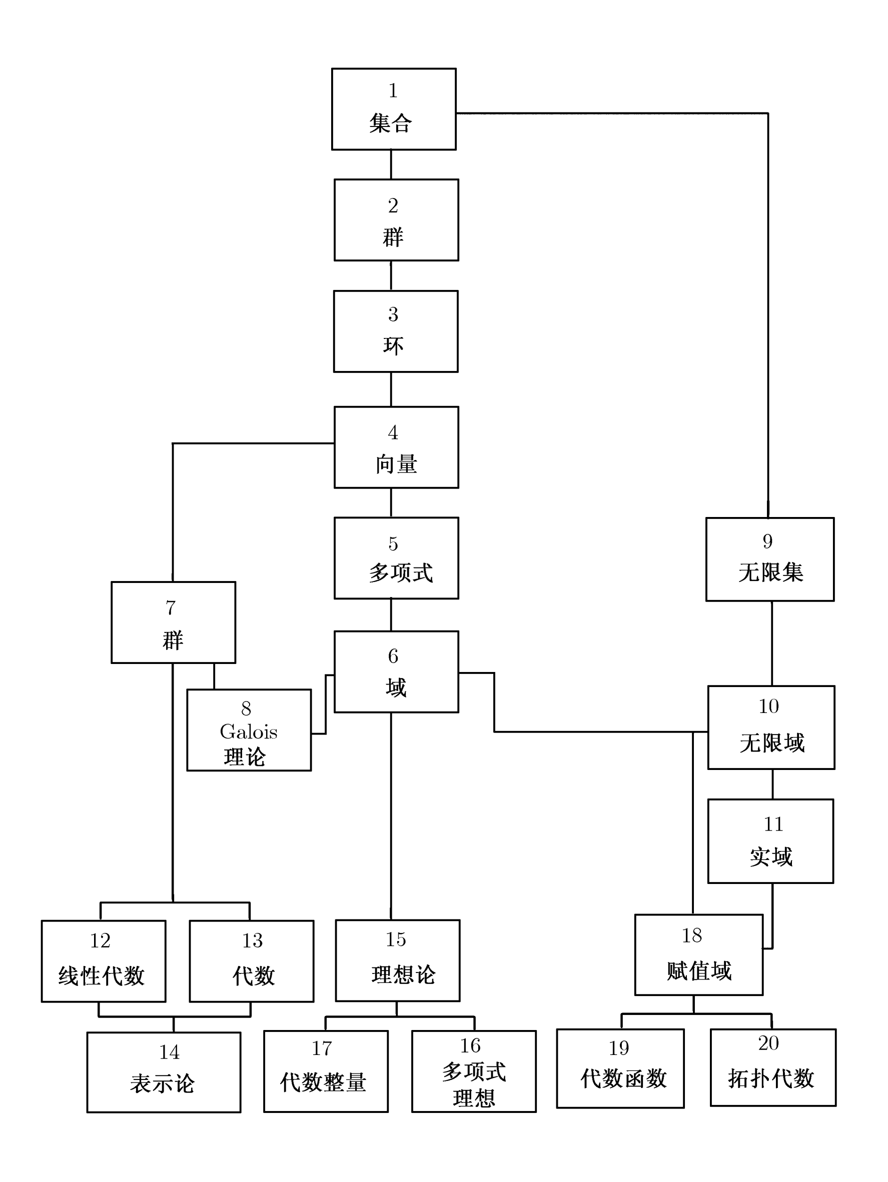
B. L. 范德瓦尔登

苏黎世, 1959 年 6 月

目　　录

全书综览图

I, II 卷中各章总览及其逻辑关系



第 12 章　线性代数

线性代数讨论模及其同态, 特别是向量空间及其线性变换. 在 12.3 节, 作为模论的应用, 证明了 Abel 群的基本定理. 12.7 节讨论二次型, 12.8 节则是反对称双线性型.

第 12 章完全建立在带算子群理论 (第 7 章) 之上.

12.1　环上的模

设 $\mathfrak{R}$ 是有单位元 ε 的环, 且设 $\mathfrak{M}$ 是右 $\mathfrak{R}$ 模, 也就是以 $\mathfrak{R}$ 作为算子集的加群. $\mathfrak{M}$ 的元素用拉丁字母表示, 而 $\mathfrak{R}$ 的元素则用希腊字母表示. 除了加群的运算外, 其他合成规则如下所示：

$$(a+b)\lambda = a\lambda + b\lambda,$$
$$a(\lambda+\mu) = a\lambda + a\mu,$$
$$a\cdot\lambda\mu = a\lambda\cdot\mu.$$

由分配律可以导出同样的对减法的规则、负号的乘法规则, 以及乘积为零时可得出其中一个因子等于零 (可以是 $\mathfrak{R}$ 的零元素或 $\mathfrak{M}$ 的零元素).

把乘法写在右方是一个随意的规定.　所有的定理对于写在左方的乘法同样正确.

$\mathfrak{R}$ 的单位元不一定是恒等算子, 对于某些 a, $a\varepsilon$ 可以不等于 a (例如, 如果规定对所有的 a 及 λ 均有 $a\lambda=0$, 那么所有的合成规则都被满足). 但是总是有

$$a = (a - a\varepsilon) + a\varepsilon, \tag{12.1}$$

其中 $a - a\varepsilon$ 被 ε 的右乘零化, 而第二项则在 ε 的右乘下不变. 第一项构成 $\mathfrak{M}$ 的子模 $\mathfrak{M}_0$, 它被 ε 零化, 从而被 $\mathfrak{R}$ 的任意元素 $\varepsilon\lambda$ 零化. 第二个因子构成子模 $\mathfrak{M}_1$, 其中 ε 是恒等算子. 这两个子模只有一个公共元, 就是零元素, 这是因为其他元素不可能同时被零化又保持不变. 表示式 (12.1) 说明了 $\mathfrak{M}$ 是直和 $\mathfrak{M}_0+\mathfrak{M}_1$. 除去 $\mathfrak{M}$ 的无趣部分 $\mathfrak{M}_0$ 后, 就能得到一个 ε 是恒等算子的模. *以后总是假设 $\mathfrak{R}$ 的单位元是 $\mathfrak{M}$ 的恒等算子.*

特别当 $\mathfrak{R}$ 是体时, $\mathfrak{M}$ 是 4.1 节意义下的 $\mathfrak{R}$ 上向量空间.

模 $\mathfrak{M}$ 称为在 $\mathfrak{R}$ 上*有限*, 如果它的元素可以表示成有限多个基元素 $u_1,\cdots,u_n$ 的线性组合：

$$u_1\lambda_1 + \cdots + u_n\lambda_n. \tag{12.2}$$

这时 $\mathfrak{M}$ 是子模 $u_1\mathfrak{R}, \cdots, u_n\mathfrak{R}$ 之和:

$$\mathfrak{M} = (u_1\mathfrak{R}, \cdots, u_n\mathfrak{R}). \tag{12.3}$$

(12.3) 也可以简写成

$$\mathfrak{M} = (u_1, \cdots, u_n).$$

如果在表示式 (12.2) 中, 系数 $\lambda_1, \cdots, \lambda_n$ 由 u 唯一确定, 就称 $\mathfrak{M}$ 是 $\mathfrak{R}$ 上的线性型模. 在这种情形, 和式 (12.3) 是直和:

$$\mathfrak{M} = u_1\mathfrak{R} + \cdots + u_n\mathfrak{R}.$$

根据 4.1 节, 有限维向量空间里总可以选取一个线性无关基 $(u_1, \cdots, u_n)$, 因此是线性型模. 由 4.2 节, 维数 n 与基的选取无关.

把线性型模 $\mathfrak{M} = (u_1, \cdots, u_m)$ 映到线性型模 $\mathfrak{N} = (v_1, \cdots, v_n)$ 的算子同态称为 $\mathfrak{M}$ 到 $\mathfrak{N}$ 内的线性变换. 如同 4.5 节, 对于变换 A, 有

$$A(x+y) = Ax + Ay,$$

$$A(x\lambda) = (Ax)\lambda.$$

变换 A 完全被它的基元素 u_k 的象确定:

$$Au_k = \sum u_i\alpha_{ik}.$$

系数 α_{ik} 构成变换 A 的矩阵.

如果 A 是从 $\mathfrak{M}$ 到 $\mathfrak{N}$ 上的一一映射, 则存在逆映射 A^{-1}, 有

$$A^{-1}A = 1 \quad 以及 \quad AA^{-1} = 1,$$

其中 1 代表恒等矩阵. 在这种情形, 映射 A 及其矩阵 (α_{ik}) 称为**可逆的**.

以后用同一个字母 A 表示线性变换 A 及其矩阵 (α_{ik}). 这并不太符合逻辑, 却是实用的.

12.2 Euclid 环中的模、不变因子

现在我们假设环 $\mathfrak{R}$ 是交换的, 并且是在 3.7 节中所述的意义下的一个 Euclid 环. 这就是说, 对环中每个元素 $a \neq 0$ 都给定了一个“绝对值” $g(a)$, 具有性质

$g(ab) \geqslant g(a)$, 并且除法程序成立. 由 3.7 节知道, $\mathfrak{R}$ 中每个理想都是主理想. 现在首先证明下面的定理.

定理 设 $\mathfrak{M}$ 是 $\mathfrak{R}$ 上的一个线性型模, 它具有基 $(u_1, \cdots, u_n)$, 那么 $\mathfrak{M}$ 中的每个子模 $\mathfrak{N}$ 也是线性型模, 它的基元素的个数最大是 n.

证 对于零模 $\mathfrak{M} = (0)$ 来说, 定理是显然的. 现在假设对于具有 $n-1$ 个基元素的模 $\mathfrak{M}$ 来说, 这个定理成立.

如果 $\mathfrak{N}$ 完全由 $u_1, \cdots, u_{n-1}$ 的线性型组成, 那么根据归纳假设, 定理中的结论成立. 如果 $\mathfrak{N}$ 包含着一个线性型 $u_1\lambda_1 + \cdots + u_n\lambda_n$, 其中 $\lambda_n \neq 0$, 则出现于这种线性型中的 λ_n 组成 $\mathfrak{R}$ 的一个理想. 这个理想必是一个主理想 (μ_n), 其中 $\mu_n \neq 0$. 这就是说, 在 $\mathfrak{N}$ 中有一个线性型 $l = u_1\mu_1 + \cdots + u_n\mu_n$, 并且对于 $\mathfrak{N}$ 中的每个线性型 $u_1\lambda_1 + \cdots + u_n\lambda_n$, 我们可以从它减去 l 的一个倍元 l_d, 使得它里面最后一个系数等于零. 相减之后余下来的是 $u_1, \cdots, u_{n-1}$ 的线性型, 它们组成 $\mathfrak{N}$ 中的一个子模. 根据归纳假设, 这个子模有一个线性无关基 $(l_1, \cdots, l_{m-1}), m-1 \leqslant n-1$. 这时 $l_1, \cdots, l_{m-1}, l$ 显然就生成 $\mathfrak{N}$.

$l_1, \cdots, l_{m-1}$ 已经线性无关. 如果有一个线性关系

$$l_1\beta_1 + \cdots + l_{m-1}\beta_{m-1} + l\beta = 0$$

成立, 其中 $\beta \neq 0$, 那么比较 u_n 的系数即有 $\mu_n\beta = 0$, 然而这是不可能的.

习题 12.1 设 $\mathfrak{M}$ 是一个整系数线性型模, $\mathfrak{N}$ 是由有限多个线性型 $v_k = \sum u_i\alpha_{ik}$ 生成的子模, 那么 $\mathfrak{N}$ 的一个具有上述性质的基 $(l_1, \cdots, l_m)$ 可以经过有限多个步骤作出.

习题 12.2 利用习题 12.1 中所作出的基 $(l_1, \cdots, l_m)$, 给出一个方法来判断一个给定的线性型 $u_1\beta_1 + \cdots + u_n\beta_n$ 是否属于模 $\mathfrak{N}$, 或者换一种说法, 判断线性丢番图 (Diophantos) 方程组

$$\sum \alpha_{ik}\xi_k = \beta_i$$

是否有整数 ξ_k 表示的解.

不变因子定理 设 $\mathfrak{N}$ 是线性型模 $\mathfrak{M}$ 的一个子模, 那么一定可以找到 $\mathfrak{M}$ 的一个基 $(u_1, \cdots, u_n)$ 和 $\mathfrak{N}$ 的一个基 $(v_1, \cdots, v_m)$, 使得

$$\begin{cases} v_i = u_i\varepsilon_i, \\ \varepsilon_{i+1} \equiv 0(\varepsilon_i). \end{cases} \tag{12.4}$$

证 我们从 $\mathfrak{M}$ 的一个任意基 $(u_1, \cdots, u_n)$ 和 $\mathfrak{N}$ 的一个任意基 $(v_1, \cdots, v_m)$ 出发. 设

$$v_k = \sum u_i\alpha_{ik}, \tag{12.5}$$

或把 (12.5) 写成矩阵形式

$$(v_1, \cdots, v_m) = (u_1, \cdots, u_n)A. \tag{12.6}$$

现在我们要逐步变换 $\mathfrak{M}$ 和 $\mathfrak{N}$ 的基, 以便将矩阵 A 化成所期望的对角线形式[①]：

$$\begin{pmatrix} \varepsilon_1 & 0 & \cdots & 0 \\ 0 & \varepsilon_2 & & \vdots \\ \vdots & & \ddots & \varepsilon_m \\ \vdots & & & \vdots \\ 0 & \cdots & & 0 \end{pmatrix}. \tag{12.7}$$

这里可容许的变换是：

(1) 交换两个 u 或两个 v, 其效果是交换 A 的两个行或两个列.

(2) 将某一 u_i 换成 $u_i + u_j\lambda (j \neq i)$. 这一变换相当于在 A 中自第 j 行减去 λ 左乘第 i 行：

$$v_k = \sum u_i \alpha_{ik} = \cdots + (u_i + u_j\lambda)\alpha_{ik} + \cdots + u_j(\alpha_{jk} - \lambda\alpha_{ik}) + \cdots.$$

(3) 将某一 v_k 换成 $v_k - v_j\lambda (j \neq k)$. 这一变换相当于在 A 中自第 k 列减去 λ 右乘第 j 列：

$$v_k - v_j\lambda = \sum u_i(\alpha_{ik} - \alpha_{ij}\lambda).$$

我们通过 (1)~(3) 来作矩阵 A 的各种可能的变换, 使得 A 中按绝对值最小的非零元素具有尽可能小的绝对值. 通过变换 (1) 可以使得矩阵中的这个最小元素处于 α_{11} 的位置上. 继此之后, 可以通过变换 (2) 从矩阵的各行中减去第一行的适当的倍, 使得第一列中其余的元素尽可能地小. 这时这些元素按绝对值来说小于 $|\alpha_{11}|$, 因而必须等于零. 同样, 通过变换 (3) 可以不改变第一个列而使得第一行中所有其余元素均为零. 经过这些操作之后, 整个矩阵中所有的元素都能被 α_{11} 整除. 事实上, 假如某一 α_{ik} 不能被 α_{11} 整除, 那么由带余除法有

$$\alpha_{ik} = \alpha_{11}\beta + \gamma, \quad \gamma \neq 0, \quad g(\gamma) < g(\alpha_{11}).$$

先通过变换 (2) 将第一行加到第 i 行上去, 然后通过变换 (3) 自第 k 列减去 β 乘第一列, 那么 (ik) 位置上就会出现 γ, 且有 $g(\gamma) < g(\alpha_{11})$. 而这是和我们对 α_{11} 所作的最小性假设相违的.

① 英文版有误. —— 译者注

这样一来, 我们的矩阵就具有如下形状：

$$\begin{pmatrix} \alpha_{11} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix},$$

这里, A' 中所有的元素都是 α_{11} 的倍元. 进一步, 我们可以保持第一行和第一列不变, 而将 A' 进行与前面对 A 所进行的操作完全相同的操作. 这样做的时候, 所有元素均能被 α_{11} 整除这一性质并不会消失. 最后 A' 将获得如下形式：

$$\begin{pmatrix} \alpha_{22} & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & A'' & \\ 0 & & & \end{pmatrix},$$

并且 A'' 中所有元素都能被 α_{22} 整除. 继续这样进行下去, 经过 m 步之后, 我们就得到所期望的标准形 (12.7). 在完成最后一步之前, 矩阵 $A, A', A'', \cdots$ 当中的某一个完全由零构成的情形是不会出现的, 因为这一情形出现就意味着某些 v_k 等于零, 而与此相反, 上述过程的每个阶段上元素 v 都组成 $\mathfrak{N}$ 的一个线性无关基. 这样就证明了这个定理.

注 (1) 操作 (1)~(3) 每次都相当于将矩阵左乘或右乘一个系数属于 $\mathfrak{R}$ 的可逆矩阵. 事实上, 如果以 $(u_1', \cdots, u_n') = (u_1, \cdots, u_n)B, (v_1', \cdots, v_m') = (v_1, \cdots, v_m)C$ 作为新的基引入, 则

$$\begin{aligned}(v_1', \cdots, v_m') &= (v_1, \cdots, v_m)C \\ &= (u_1, \cdots, u_n)AC = (u_1', \cdots, u_n')B^{-1}AC.\end{aligned}$$

这样一来, 初等因子定理就相当于说, 存在两个可逆方阵 B, C, 使得 $B^{-1}AC$ 具有形式 (12.7).

(2) 当 v 不是一组线性无关的元素时, 矩阵 A 化为标准形的过程也可以按完全同样的方法进行, 只不过在这一情形下矩阵 $A, A', A'', \cdots$ 当中有一个可能为零矩阵, 这时所得到的不是标准形 (12.7), 而是较一般的形式

$$B^{-1}AC = \begin{pmatrix} \varepsilon_1 & & & 0 \\ & \ddots & & \\ & & \varepsilon_r & \\ 0 & & & 0 \end{pmatrix}, \tag{12.8}$$

其中 r 是 A 的秩. ε_i 之间的可除性关系仍然被保持.

(3) 大家知道, 变换后的矩阵 $D = B^{-1}AC$ 中的 k 阶子行列式是 A 的子行列式的线性函数. 同样, $A = BDC^{-1}$ 的子行列式是 D 的子行列式的线性函数. 因此, A 的 k 阶子行列式的最大公因子 δ_k 除了相差一个可逆元素之外, 和 D 的 k 阶子行列式的最大公因子相同. 对于 D 来说, 我们很容易计算出 δ_k 的值：

$$\delta_k = \varepsilon_1\varepsilon_2\cdots\varepsilon_k, \quad k \leqslant r.$$

因此

$$\delta_k = \delta_{k-1}\varepsilon_k, \quad 1 < k \leqslant r. \tag{12.9}$$

δ_k 叫做矩阵 A 的行列式因子, 而 ε_k 则叫做矩阵 A 的不变因子. 由 (12.9) 可知：不变因子等于相邻的两个行列式因子的商.

(4) 不变因子 ε_k 除了相差一个可逆元素外, 由矩阵 A 唯一确定. 这一事实在下一节里将要通过另一途径得出. 在下一节里将要证明, 不变因子 (只要它们不是可逆元素) 只与商模 $\mathfrak{M}/\mathfrak{N}$ 有关, 而这个商模显然由 A 完全确定[1].

习题 12.3 每一个具有整数系数 α_{ik} 和常数项 β_i 的线性丢番图方程组

$$\sum_1^n \alpha_{ik}\xi_k = \beta_i, \quad i = 1, \cdots, m \tag{12.10}$$

都可以通过未知量和方程的幺模变换变成

$$\begin{aligned} &\varepsilon_i\eta_i = \gamma_i, \quad i = 1, \cdots, r; \varepsilon_i \neq 0, \\ &0 = \delta_j, \quad j = r+1, \cdots, m \end{aligned}$$

的形式. 这个方程组有整数解的条件是

$$\gamma_i \equiv 0(\varepsilon_i), \quad \delta_j = 0.$$

当 $i \leqslant r$ 时, 相应的 η_i 可由上述条件确定, 而其余的 η_j 则是任意的. ξ_k 是这些任意的 η_j 的带有整系数的线性函数.

12.3 Abel 群的基本定理

设 $\mathfrak{G}$ 是一个具有有限多个生成元的、写成加群形式的 Abel 群, 也就是一个模. 如果给出了 $\mathfrak{G}$ 的一个算子区 $\mathfrak{R}$, 我们总是认为 $\mathfrak{R}$ 中有一个单位元, 并且这个单位

[1] 原书不区分不变因子和初等因子, 统称初等因子. 为了方便读者, 我们作了不同的翻译. —— 中译者注

元就是单位算子. 如果没有给出 $\mathfrak{G}$ 的算子区, 那么就认为整数环是算子区, 这个算子区同样满足上述假定. 这一次我们把算子写在模元素的左边.

先设 $\mathfrak{G}$ 是一个循环群：$\mathfrak{G}=(g)$. $\mathfrak{R}$ 中将 g 零化的元素 μ 的全体是 $\mathfrak{R}$ 中的一个左理想 $\mathfrak{a}$：由 $\mu_1 g=0$ 和 $\mu_2 g=0$ 即有 $(\mu_1-\mu_2)g=0$, 并且由 $\mu g=0$ 即可知, 对于 $\mathfrak{R}$ 中每个 κ 都有 $\kappa\mu g=0$. 对于 $\mathfrak{R}$ 中的每个 λ, 令 λg 与它对应. 由于

$$(\lambda+\mu)g=\lambda g+\mu g,$$
$$\lambda\mu\cdot g=\lambda\cdot\mu g,$$

所以这一对应是一个对于 $\mathfrak{R}$ 的算子同态. 根据同态定理即有

$$\mathfrak{G}\cong\mathfrak{R}/\mathfrak{a},$$

或者说, 一个循环 $\mathfrak{R}$ 模 $\mathfrak{G}$ 与 $\mathfrak{R}$ 对于 $\mathfrak{G}$ 的零化左理想的同余类模同构.

对于普通循环群 $\mathfrak{G}$ 的情形, 从这里可以重新得到过去已有的结果, 即 $\mathfrak{G}$ 与整数加群或对某一整数的同余类群同构. 如果理想 $\mathfrak{a}$ 的基元素是 $n>0$, 则循环群 (g) 或元素 g 的阶等于 n.

刚才所证明的定理并不依赖于我们对 $\mathfrak{R}$ 所作的各种特殊假设. 如果像我们以下将要假定的那样, $\mathfrak{R}$ 是交换的并且是一个 Euclid 环, 那么还可以得出更进一步的结论. 这时理想 $\mathfrak{a}$ 是一个主理想：$\mathfrak{a}=(\alpha)$. 我们假设 $\alpha\neq 0$, 并且 (如果可能的话) 将 α 分解成两个互素的因子：

$$\alpha=\rho\sigma,$$
$$1=\lambda\rho+\mu\sigma,$$

然后作出循环群 $\mathfrak{G}_1=(\rho g),\mathfrak{G}_2=(\sigma g)$. 这时 $\mathfrak{G}_1$ 被 σ 所零化而 $\mathfrak{G}_2$ 被 ρ 所零化. 由于

$$g=\lambda\rho g+\mu\sigma g,$$

所以 $\mathfrak{G}$ 是 $\mathfrak{G}_1$ 和 $\mathfrak{G}_2$ 的和. 交 $\mathfrak{G}_1\bigcap\mathfrak{G}_2$ 被 ρ 和 σ 所零化, 从而被 $1=\lambda\rho+\mu\sigma$ 所零化. 因此 $\mathfrak{G}_1\bigcap\mathfrak{G}_2=(0)$, 从而两个子群之和是直和：

$$\mathfrak{G}=\mathfrak{G}_1+\mathfrak{G}_2.$$

如果 σ 或 ρ 还可以进一步分解成互素的因子, 则 $\mathfrak{G}_1$ 或 $\mathfrak{G}_2$ 还可以进一步分解. 循环群 $\mathfrak{G}$ 最后将被分解成一些循环群的直和, 其中每个直因子被一个素数幂[①]所零化. 这些素数幂的乘积等于 α. 具有这一性质的群称为素数幂群.

① “素数”一词是“环 $\mathfrak{R}$ 中的素元”的简称. 在普通 Abel 群的情形就是普通的素数.

现在我们转向一般的情形. 这时 $\mathfrak{G}$ 是一个具有有限多个生成元 $g_1, \cdots, g_n$ 的 $\mathfrak{R}$ 模, 因而 $\mathfrak{G}$ 中的元素具有形式：

$$\lambda_1 g_1 + \cdots + \lambda_n g_n.$$

如果我们作出不定元 $u_1, \cdots, u_n$ 的线性型模

$$\mathfrak{M} = (u_1, \cdots, u_n),$$

则 $\mathfrak{M}$ 中的每个线性型 $\sum \lambda_i u_i$ 有 $\mathfrak{G}$ 中的一个元素 $\sum \lambda_i g_i$ 与之对应. 这个对应是一个模同态, 因而根据同态定理有

$$\mathfrak{G} \cong \mathfrak{M}/\mathfrak{N},$$

其中 $\mathfrak{N}$ 是那样一些线性型 $\sum \lambda_i u_i$ 组成的子模, 对于它们来说, $\sum \lambda_i g_i = 0$.

我们仍旧假定 $\mathfrak{R}$ 是一个 Euclid 环. 根据 12.2 节, 可以引入 $\mathfrak{N}$ 和 $\mathfrak{M}$ 的新基 $(v_1, \cdots, v_m)$ 和 $(u'_1, \cdots, u'_n)(n \geqslant m)$, 使得

$$\begin{aligned} &v_i = \varepsilon_i u'_i, \quad i = 1, \cdots, m, \\ &\varepsilon_{i+1} \equiv 0(\varepsilon_i). \end{aligned}$$

在上面所定义的同态之下, 基元素 u' 被映成 $\mathfrak{G}$ 中的元素 $h_1, \cdots, h_n$. $\mathfrak{G}$ 中所有元素都具有 $\mu_1 h_1 + \cdots + \mu_n h_n$ 的形式, 并且这样一个元素等于零, 当且仅当

$$\mu_1 u'_1 + \cdots + \mu_n u'_n \equiv 0(v_1, \cdots, v_m),$$

即

$$\left\{\begin{array}{l} \mu_1 \equiv 0(\varepsilon_1), \\ \cdots\cdots\cdots \\ \mu_m \equiv 0(\varepsilon_m) \end{array}\right. \qquad \left\{\begin{array}{l} \mu_{m+1} = 0, \\ \cdots\cdots\cdots \\ \mu_n = 0. \end{array}\right.$$

这就是说, 一个和 $\mu_1 h_1 + \cdots + \mu_n h_n$ 等于零, 当且仅当它们的各个单项等于零; 而各单项等于零, 当且仅当它们的系数 μ_i 在 $i = 1, \cdots, m$ 时能被 ε_i 整除, 而在 $i = m+1, \cdots, n$ 时等于零.

另一种表述方式是:

定理　*群 $\mathfrak{G}$ 是一些循环群的直和: $\mathfrak{G} = (h_1) + \cdots + (h_n)$, 而 (h_i) 的零化理想是*

$$\begin{aligned} &(\varepsilon_i), \quad \text{当 } i = 1, \cdots, m, \\ &(0), \quad \text{当 } i = m+1, \cdots, n. \end{aligned}$$

这就是具有有限多个生成元的 Abel 群的基本定理.

在普通 Abel 群的情形, $|\varepsilon_i|$ 就是循环群 $(h_1),\cdots,(h_m)$ 的阶, 而其余的循环群 $(h_{m+1}),\cdots,(h_n)$ 则是无限的.

对于基本定理还需要作以下三点补充:

(1) 去掉不变因子 ε_i 中的可逆元素;

(2) 将循环群进一步分解为素数幂群;

(3) 唯一性.

(1) 如果 ε_1 是一个可逆元素, 那么 (ε_1) 就是单位理想, 因而 $\mathfrak{R}h_1=(0)$. 这时循环群 $\mathfrak{R}h_1$ 可以从直分解 $\mathfrak{R}h_1+\cdots+\mathfrak{R}h_n$ 中除去.

去掉所有的可逆元素之后, 可将余下来的零化理想 $(\varepsilon_i),(0)$ 按照相反的顺序排列成 $\mathfrak{a}_1,\cdots,\mathfrak{a}_q$. 这时就有

$$\mathfrak{a}_i\equiv 0(\mathfrak{a}_{i+1}).$$

(2) 循环群 (h_i) 当中, 其零化理想为 (0) 者与 $\mathfrak{R}$ 同构. 另一方面, 根据本节开头所证明的, 零化理想 $(\varepsilon_i)\neq(0)$ 的循环群还可以进一步分解为素数幂群. 相应的零化素数幂可由 ε_i 的因子分解得出. 在 $\mathfrak{G}$ 的分解中属于同一素数 p 的素数幂群之和是一个子群 $\mathfrak{B}_p$, 这个子群由 $\mathfrak{G}$ 中能被一个适当高的幂 p^ρ 所零化的元素组成. 因此群 $\mathfrak{B}_p$ 是唯一确定的. 如果命 $\mathfrak{A}$ 表示零化理想为 (0) 的循环群之和, 那么就有

$$\mathfrak{G}=\sum_p\mathfrak{B}_p+\mathfrak{A}.$$

将 $\mathfrak{B}_p$ 作进一步的分解, 我们又可以反过来得出素数幂群. 这些素数幂群不是绝对地唯一确定的, 但在下面可以看到, 它们是在相差一个同构的意义下唯一确定的. 另一方面, 每个 $\mathfrak{B}_p$ 中有一个唯一确定的子群列 $\mathfrak{B}_{p,\rho},\mathfrak{B}_{p,\rho-1},\cdots,\mathfrak{B}_{p,0}$, 其中 $\mathfrak{B}_{p,\nu}$ 由群 $\mathfrak{B}_p$ 中所有能被 p^ν 零化的元素组成. 这个子群列中第一个子群是 $\mathfrak{B}_p$, 最后一个子群仅含一个元素零.

群 $\mathfrak{A}$ 不是唯一确定的, 但在相差一个同构的意义下是唯一确定的, 因为我们有

$$\mathfrak{A}\cong\mathfrak{G}/\sum_p\mathfrak{B}_p.$$

(3) **唯一性定理**. *在直分解 $\mathfrak{G}=\mathfrak{G}_1+\cdots+\mathfrak{G}_q$ 中出现的满足条件 $\mathfrak{a}_i\equiv 0(\mathfrak{a}_{i+1})$ 的零化理想 $\mathfrak{a}_1,\cdots,\mathfrak{a}_q$ 由模 $\mathfrak{G}$ 本身唯一确定 (或等价地, 群 $\mathfrak{G}_i$ 被唯一确定到相差同构).*

证 如果能够证明, 对于 $\mathfrak{R}$ 中每个素数幂 p^σ, 可以唯一地判定它能整除多少个 $\mathfrak{a}_i$, 那么定理中所断言的唯一性就证明了. 事实上, 如果 p^σ 恰能整除这些理想当中的 k 个, 那么由于这些理想本身之间的可除性关系, 能被 p^σ 所整除的就是开

头的 k 个理想, 即 $\mathfrak{a}_1, \cdots, \mathfrak{a}_k$. 这样一来, 对于每个素数幂 p^σ 来说, 我们不但知道它能够整除多少个 $\mathfrak{a}_i$, 而且还知道它能够整除哪些个 $\mathfrak{a}_i$. 因而对于每一个 $\mathfrak{a}_i$ 来说, 就知道它能被哪些素数幂所整除. 能够被任意高次幂整除的 $\mathfrak{a}_i$ 就是零理想, 而其余的理想则由它们的素因子分解唯一地确定.

如果 p^σ 整除循环群 $\mathfrak{G}_i$ 的零化理想 $\mathfrak{a}_i$, 则

$$p^{\sigma-1}\mathfrak{G}_i/p^\sigma\mathfrak{G}_i$$

是一个以 (p) 为零化理想的循环群, 因而是一个单群. 与此相反, 如果 p^σ 不能整除 $\mathfrak{a}_i$, 则 $p^\sigma\mathfrak{G}_i = p^{\sigma-1}\mathfrak{G}_i$, 从而 $p^{\sigma-1}\mathfrak{G}_i/p^\sigma\mathfrak{G}_i = (0)$. 因此 $p^{\sigma-1}\mathfrak{G}/p^\sigma\mathfrak{G}$ 是一些单群的直和, 这些单群的个数等于能够被 p^σ 整除的 $\mathfrak{a}_i$ 的个数 k. 这样一来, k 就是 $p^{\sigma-1}\mathfrak{G}/p^\sigma\mathfrak{G}$ 的合成列的长度, 因而是唯一确定的.

习题 12.4 将最后这个证明中最后简略写出的部分补充完全.

习题 12.5 在 (2) 中作出的群 $\mathfrak{A}$ 是整数环 $\mathbb{Z}$ 上的一个线性型模, 它所能分解成的循环群的个数等于群 $\mathfrak{G}$ 的秩 (秩 = 对 $\mathfrak{R}$ 线性无关的元素的最大个数).

习题 12.6 考虑 (2) 中所作出的唯一确定的群及其商群的合成列的长度, 从而给出唯一性定理的另一证明. 模 $\mathfrak{A}$ 的秩 (见习题 12.5) 也可以利用.

12.4 表示与表示模

设 K 是体. 所谓环 $\mathfrak{o}$ 在 K 上的一个线性变换或方阵表示, 指的是一个同态

$$\mathfrak{o} \sim \mathfrak{O},$$

其中 $\mathfrak{O}$ 是 K 中的 r 阶方阵所组成的一个环. 如果这个同态是一个同构, 我们就说这个表示是一个忠实表示.

环 $\mathfrak{o}$ 在 K 上的一个表示模就是这样一个 “双模” $\mathfrak{M}$, 它以 $\mathfrak{o}$ 为左算子区, 以 K 为右算子区, 并且具有下列性质:

(1) $\mathfrak{M}$ 可以看成 K 上的一个线性型模:

$$\mathfrak{M} = u_1K + \cdots + u_nK.$$

(2) 对于 $a \in \mathfrak{o}, u \in \mathfrak{M}, \lambda \in K$, 有

$$a \cdot u\lambda = au \cdot \lambda. \tag{12.11}$$

后一要求说明, 以 a 去乘 $\mathfrak{M}$ 中的元素是 K 模 $\mathfrak{M}$ 的一个算子同态, 即一个线性变换. 这个线性变换可由一个方阵 $A = (\alpha_{ik})$ 给出:

$$a \cdot u_k = \sum u_j\alpha_{jk},$$

$$a \cdot \sum u_k \lambda_k = \sum \sum u_j \alpha_{jk} \lambda_k. \tag{12.12}$$

这样一来. 对于 $\mathfrak{o}$ 中每个元素 a, 有 K 中的一个方阵 A 与它对应. 由于我们对模 $\mathfrak{M}$ 所作的假设, 与 $\mathfrak{o}$ 中两个元素 a, b 之和与积相对应的是相应的线性变换的和与积, 因而也是相应的方阵的和与积. 因此, 对应 $a \to A$ 是环 $\mathfrak{o}$ 的一个表示.

反之, 如果给出了环 $\mathfrak{o}$ 在 K 上的一个线性型模 $\mathfrak{M}$ 中的线性变换表示, 那么只要通过 (12.12) 来定义乘积 $a \cdot u (a \in \mathfrak{o}, u \in \mathfrak{M})$, 就可以使 $\mathfrak{M}$ 成为一个双模. 这时我们可以反过来证明双模的一切性质以及规律 (12.11) 成立. 因此, $\mathfrak{M}$ 是一个表示模.

相应于每个表示模有环 $\mathfrak{o}$ 的一个线性变换表示, 或者当我们选定一个 K 基 $(u_1, \cdots, u_n)$ 之后, 有一个方阵表示. 反之, 相应于每个表示有一个表示模.

当我们通过基变换

$$(u_1', \cdots, u_n') = (u_1, \cdots, u_n) P$$

由基 $(u_1, \cdots, u_n)$ 过渡到另一基 $(u_1', \cdots, u_n')$ 时, 同一线性变换由方阵

$$A' = P^{-1} A P$$

给出. 这时与环中的元素 a 相对应的就是一个新的方阵 A'. 我们说这是一个等价表示. 因为由一个表示过渡到一个与之等价的表示只不过是由表示模的一个基过渡到同一表示模 (或一个与之算子同构的模) 的另一个基, 所以得出如下的结论: 等价的表示相当于彼此同构的表示模, 反之亦然.

线性型模 $\mathfrak{M}$ 的一组线性变换, 特别是一个环的一个表示, 叫做可约的, 如果这一组里的所有线性变换都将某一固定的线性子空间 $\mathfrak{N} \neq (0), \neq \mathfrak{M}$ 映入它自身之内. 这时 $\mathfrak{N}$ 叫做一个不变子空间. 当我们所考虑的是某一环 $\mathfrak{o}$ 的一个表示时, 将 $\mathfrak{M}$ 看成对于 $\mathfrak{o}$ 和 K 的一个双模, 那么不变子空间 $\mathfrak{N}$ 能够容许 $\mathfrak{o}$ 的一切元素作为左算子. 由此可知, 环的一个表示是可约的, 当且仅当相应的表示模有一个子 (双) 模 $\mathfrak{N}$.

为了研究一个可约表示的方阵具有何种形状, 我们从 $\mathfrak{N}$ 的一个 K 基出发, 并将其扩充为 $\mathfrak{M}$ 的一个 K 基. 现在设

$$\begin{aligned} \mathfrak{N} &= v_1 K + \cdots + v_r K, \\ \mathfrak{M} &= v_1 K + \cdots + v_r K + w_1 K + \cdots + w_t K. \end{aligned}$$

一个线性变换将 $\mathfrak{N}$ 映入它自身之内这一事实, 总意味着元素 v 经过变换后所得的元素仍可由 v 表出, 即有

$$v_j' = \sum v_i \rho_{ij},$$

$$w'_j = \sum v_i\sigma_{ij} + \sum w_i\tau_{ij}. \tag{12.13}$$

令 $R = (\rho_{ij}), S = (\sigma_{ij}), T = (\tau_{ij})$, 则线性变换由方阵

$$A = \begin{pmatrix} R & S \\ 0 & T \end{pmatrix} \tag{12.14}$$

给出. 由此可知, 一组方阵是可约的, 当且仅当这一组的所有方阵都能够由一个变换 $A' = P^{-1}AP$(即选择一个新基) 同时化为 (12.14) 的形式.

由 (12.13) 可以看出,

$$\begin{aligned}(v'_1 \cdots v'_r) &= (v_1 \cdots v_r) \cdot R,\\ (w'_1 \cdots w'_t) &\equiv (w_1 \cdots w_t) \cdot T \pmod{\mathfrak{N}}.\end{aligned} \tag{12.15}$$

这个式子可以作如下解释:

对环 $\mathfrak{o}$ 的一个可约表示来说, 如果把不变子模 $\mathfrak{N}$ 和商模 $\mathfrak{M}/\mathfrak{N}$ 都看成表示模, 那么由这两个模得到的表示由 (12.14) 中的两部分 R 和 T 给出.

如果取 $\mathfrak{N}$ 为一个最大不变子模 $\mathfrak{M}_{l-1}$, 而在这一子模中又取一个最大不变子模 $\mathfrak{M}_{l-2}$ 等等, 直到得出一个合成列

$$\mathfrak{M} = \mathfrak{M}_l,\ \mathfrak{M}_{l-1}, \cdots, \mathfrak{M}_0 = (0),$$

那么适当地选取 $\mathfrak{M}$ 的基之后, 表示的方阵就具有如下形式:

$$\begin{pmatrix} R_{11} & \cdots & & R_{1l} \\ 0 & R_{22} & & \vdots \\ \vdots & & \ddots & \\ 0 & \cdots & 0 & R_{ll} \end{pmatrix}. \tag{12.16}$$

对角线上的方块 R_{ii} 给出与合成因子 $\mathfrak{M}_i/\mathfrak{M}_{i-1}$ 相当的表示. 由于这些合成因子都是一些单纯双模 (即没有不变子模), 所以相应的表示都是不可约的. 将一个表示化成 (12.16) 这种形式的过程称为表示的"约化过程". 根据 Jordan-Hölder 定理 (7.4 节), 合成因子除了次序之差外, 在相差一个算子同构的意义下是唯一确定的. 因此, 约化后的表示 (12.16) 中, 不可约成分 R_{ii} 除了次序之差外, 在等价表示的意义下是唯一确定的.

如果在 (12.13) 中, σ_{ij} 都等于零, 那么这就意味着不仅 $(v_1, \cdots, v_r)$ 是一个不变子模, 而且 $(w_1, \cdots, w_t)$ 也是一个不变子模. 因此 $\mathfrak{M}$是两个不变子模 $\mathfrak{N}$ 与 $\mathfrak{Q}$ 的

直和. 这时方阵 (12.14) 具有形式

$$A = \begin{pmatrix} R & 0 \\ 0 & T \end{pmatrix},$$

其中 R 属于由 $\mathfrak{N}$ 所确定的表示, T 属于由 $\mathfrak{Q}$ 所确定的表示. 在这一情形下就说, 表示 $a \to A$**分解成**表示 $a \to R$ 和 $a \to T$.

如果双模 $\mathfrak{M}$ 在 7.6 节的意义下完全可约, 也就是说, 可以分解成一些单纯双模的直和, 则由 $\mathfrak{M}$ 所确定的表示由方阵

$$\begin{pmatrix} R_{11} & & & 0 \\ & R_{22} & & \\ & & \ddots & \\ 0 & & & R_{ll} \end{pmatrix} \tag{12.17}$$

给出. 对角线上的方块给出一些不可约表示, 其中当然可能有相同的表示出现. 我们把这样一个表示称为**完全可约的**.

下面几节中关于单个方阵的理论给出了本节中各种概念的例子.

习题 12.7 设 $\mathfrak{o}$ 是一个具有单位元素的环, 并且在 $\mathfrak{o}$ 的一个表示下单位元素被映成单位方阵, 那么对于相应的表示模来说, 单位元素即单位算子. 利用 12.1 节中的一个定理证明, $\mathfrak{o}$ 的每个表示可分解成两个这样的表示, 对于其中一个表示来说, 单位元素被映成单位方阵, 而在另一个表示下, 每个元素都被映成零方阵:

$$A = \begin{pmatrix} s & 0 \\ 0 & 0 \end{pmatrix}.$$

习题 12.8 一个表示是完全可约的, 当且仅当对于每一个不变子空间 $\mathfrak{N}$, 可以找到另一个不变子空间 $\mathfrak{Q}$, 使得 $\mathfrak{N}$ 和 $\mathfrak{Q}$ 一起张成空间 $\mathfrak{M}$:

$$\mathfrak{M} = \mathfrak{N} + \mathfrak{Q}.$$

习题 12.9 如果 $(u'_1, \cdots, u'_n) = (u_1, \cdots, u_n)P$ 是表示模到它自身内的一个同态, 则方阵 P 与表示中的所有方阵 A 可交换:

$$AP = PA,$$

反之亦然.

12.5　交换域中一个方阵的标准形

设 $\mathfrak{M}=(u_1,\cdots,u_n)$ 是一个交换域 K 上的一个线性型模, 而

$$u_k \to v_k = \sum u_i \alpha_{ik}$$

是 $\mathfrak{M}$ 到它自身内的一个线性变换. 我们要引入一个新的基

$$(u'_1,\cdots,u'_n)=(u_1,\cdots,u_n)P$$

(其中 P 是 K 中一个可逆方阵), 以便将方阵 $A=(\alpha_{ik})$ 化成尽可能简单的标准形式

$$A'=P^{-1}AP.$$

我们现在把方阵 A 的各次幂看作是不定元 x 的各次幂的表示, 并且对每个多项式

$$f(x)=\sum \alpha_\nu x^\nu,$$

使方阵

$$f(A)=\sum \alpha_\nu A^\nu$$

与之对应, 从而将这一表示开拓成多项式环 $K[x]$ 的一个表示. 由于 A 的各个幂相互可交换, 并且它们与系数 α_ν 也可交换, 所以这个表示是一个同态.

这个表示有一个表示模 $\mathfrak{M}$. 只要通过

$$\left(\sum \alpha_\nu x^\nu\right)u=\sum \alpha_\nu A^\nu u$$

来定义 $K[x]$ 中一个多项式与一个 $u\in\mathfrak{M}$ 的乘积就可以得出这个表示模来. 表示模 $\mathfrak{M}$ 是相对于 $K[x]$ 和 K 的一个双模. 然而 K 中的元素与所有其余元素可交换并且这些元素彼此也可交换, 因此我们可以把这些元素写在 $\mathfrak{M}$ 中的元素的左边, 即

$$u\lambda=\lambda u.$$

于是就可以直截了当地将 $\mathfrak{M}$ 看成一个 $K[x]$ 模.

由于多项式环 $K[x]$ 是一个 Euclid 环, 所以 12.3 节中的基本定理可以应用：模 $\mathfrak{M}$ 是一些循环 $K[x]$ 模 $(w_1),\cdots,(w_r)$ 的直和, 每个这样的模的零化理想或者是零理想, 或者是由 $K[x]$ 中一个多项式生成. 零理想的情形实际上是不可能的. 事实上, 对每个 $w=w_\nu$ 来说, $w,xw,x^2w,\cdots$ 诸量当中最多只可能有 n 个是线性无关的, 因此可以找到一个多项式 $\sum \alpha_\mu x^\mu \neq 0$, 使得

$$\sum \alpha_\mu x^\mu w=0.$$

这样一来, 每个 $w = w_\nu$ 都有一个次数最低的零化多项式

$$f_\nu(x) = f(x) = x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_0,$$

并且

$$f_{\nu+1}(x) \equiv 0(f_\nu).$$

元素 $w, xw, \cdots, x^{k-1}w$ 在 K 上线性无关, 因而可以用来作为循环 $K[x]$ 模 $(w) = (w, xw, x^2w, \cdots)$ 的一个基. 这样一来, 我们就有

$$\begin{gathered} Aw = xw, \\ Axw = x^2w, \\ \cdots\cdots\cdots \\ Ax^{k-1}w = x^kw = -\alpha_0 \cdot w - \alpha_1 \cdot xw - \cdots - \alpha_{k-1} \cdot x^{k-1}w, \end{gathered}$$

从而模 $(w, xw, \cdots)$ 到它自身内的变换 A 在新的基中由方阵

$$A_\nu = \begin{pmatrix} 0 & & \cdots\cdots & 0 & -\alpha_0 \\ 1 & 0 & \cdots & 0 & -\alpha_1 \\ 0 & 1 & & \vdots & \vdots \\ \vdots & & \ddots & & \\ 0 & & \cdots & 1 & -\alpha_{k-1} \end{pmatrix} \tag{12.18}$$

表示. 这种方阵称为**相伴方阵**. 对于每一 w_ν, 有一个这种类型的相伴方阵与之对应. 由于 $\mathfrak{M}$ 是 (w_ν) 的直和, 于是就得到方阵 A 的**第一标准形**:

$$A = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix}, \tag{12.19}$$

其中的小块 A_ν **都是形如** (12.18) **的相伴方阵.**

由 12.3 节中的唯一性定理可知, 多项式 $f_\nu(x)$, 从而相伴方阵 A_ν, 由模 $\mathfrak{M}$ **唯一确定.**

如果我们将循环模 (w_ν) 进一步分解成一些以素多项式的幂为零化多项式的循环模的直和, 那么 (12.19) 中的块 A_ν 还可以进一步“约化”. 这时 (12.19) 的形状仍然不变, 只不过现在的相伴方阵 (12.18) 对应于素多项式的幂 $(p(x))^\rho$(**第二标准形**).

在这一情形下的相伴方阵除了它们在 (12.19) 中的次序外, 也是唯一确定的. 多项式 $(p(x))^\rho$ 称为方阵 A 的*初等因子*.

利用循环模 (w_v) 的合成列, 我们还可以将刚才所建立的标准形作进一步的约化. 在这里我们仅就所出现的素多项式 $p(x)$ 均为一次多项式的情形来进行这样的约化. 特别当域 K 是代数封闭域时, 一定会出现这样的情形. 设

$$p(x) = x - \lambda, \quad f(x) = (x-\lambda)^\rho.$$

我们取

$$\begin{aligned} v_1 &= (x-\lambda)^{\rho-1}w, \\ v_2 &= (x-\lambda)^{\rho-2}w, \\ &\cdots\cdots\cdots \\ v_\rho &= w. \end{aligned}$$

于是

$$\begin{aligned} &(x-\lambda)v_1 = 0, \\ &(x-\lambda)v_\mu = v_{\mu-1} \quad (1 < \mu \leqslant \sigma) \end{aligned}$$

或

$$\begin{aligned} Av_1 &= xv_1 = \lambda v_1, \\ Av_\mu &= xv_\mu = \lambda v_\mu + v_{\mu-1}. \end{aligned} \tag{12.20}$$

这样一来, 块 A_1 就有“约化”形式

$$A_1 = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & & 0 & \lambda \end{pmatrix}.$$

由于对每个 w_ν 都有一个 λ_ν, 所以

$$A_\nu = \begin{pmatrix} \lambda_\nu & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ & & & 1 \\ 0 & \cdots & & \lambda_\nu \end{pmatrix}.$$

将这些块放到 (12.19) 中去, 就得到*第三标准形*. 在这里“特征根 λ_ν”和块的阶数 ρ_ν 也是唯一确定的.

对应于同一根 λ 的所有向量 v_μ 生成一个模 $\mathfrak{B}_v$, 这个模被 $x-\lambda$ 的一个幂所零化 (12.3 节). 用向量的语言来说, 这个模称为属于根 λ 的子空间. 整个模 $\mathfrak{M}$ 是这些子空间的直和. 在每个这样的子空间中我们可以作出 12.3 节中所提到的被 $(x-\lambda)^\rho, (x-\lambda)^{\rho-1}, \cdots, 1$ 所零化的子空间列. 被 $x-\lambda$ 所零化, 也就是说, 满足条件

$$Aw = \lambda w$$

的向量 w, 称为方阵 A 的属于特征值 λ 的特征向量.

当所有的 ρ 都等于 1, 也就是说, 当多项式 $f_\nu(x)$ 没有重因子时, 我们就得到完全可约的情形 (参看 12.4 节), 这时标准形 (12.19) 具有对角线形式

$$\begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}. \tag{12.21}$$

又因为

$$f_{\nu+1} \equiv 0(f_\nu),$$

所以只要最高次的初等因子 $f_r(x)$ 没有重因子就够了.

关于求特征根和建立标准形的实际方法将在下一节中给出.

习题 12.10 最高次不变因子 $f_r(x)$ 可以刻画作为具有性质

$$f(x)\mathfrak{M} = 0 \quad 或 \quad f(A) = 0$$

的次数最低的多项式.

习题 12.11 设方阵 A 已表成第二或第三种标准形, 试决定与 A 可交换的方阵的全体 (参看习题 12.9).

12.6 不变因子与特征函数

在变换

$$A' = P^{-1}AP$$

之下, 方阵 $xE-A$ 变成

$$P^{-1}(xE-A)P = xP^{-1}EP - P^{-1}AP = xE - A'.$$

我们要决定在 12.2 节的意义之下, 方阵 $xE-A$ 在 $K[x]$ 中的不变因子. 由于左乘和右乘一个可逆方阵时, 这些不变因子是不变的, 因此可以只决定方阵 $xE-A'$ 的

不变因子, 这里 A' 是 12.5 节中的第一标准形. 由 (12.18) 和 (12.19) 可知, $xE - A'$ 由形如

$$xE_1 - A_1 = \begin{pmatrix} x & 0 & \cdots & 0 & \beta_0 \\ -1 & x & & \vdots & \vdots \\ 0 & \ddots & \ddots & & \\ \vdots & \ddots & & x & \beta_{h-2} \\ 0 & \cdots & 0 & -1 & x+\beta_{h-1} \end{pmatrix}$$

的块组成. 为了决定这个方阵的不变因子, 我们要把它化成对角线形式. 将第二至第 h 行分别乘以 $x, x^2, \cdots, x^{h-1}$, 加到第一行上去, 就得到

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & f(x) \\ -1 & x & & \vdots & \beta_1 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & & x & \beta_{h-2} \\ 0 & \cdots & 0 & -1 & x+\beta_{h-1} \end{pmatrix}.$$

经过行的对换将第一行移到最下面来, 那么主对角线以下全都是零. 再将前面的列的适当倍加到后面的列上去, 很容易使主对角线以上全变为零. 这样就得到

$$\begin{pmatrix} -1 & & & & 0 \\ & -1 & & & \\ & & \ddots & & \\ & & & -1 & \\ 0 & & & & f(x) \end{pmatrix}.$$

最后, 把所有这样的块排列起来, 并且交换行和列的次序, 使得在主对角线上先出现所有的 -1, 那么就得到所寻求的对角线形式

$$\begin{pmatrix} -1 & & & & & & 0 \\ & -1 & & & & & \\ & & \ddots & & & & \\ & & & -1 & & & \\ & & & & f_1(x) & & \\ & & & & & \ddots & \\ 0 & & & & & & f_r(x) \end{pmatrix}.$$

这样一来, 我们就看到, 多项式 $f_\nu(x)$ 连同某些 1 一起是 $xE-A$ 的不变因子.

A 的特征多项式 (特征函数)

$$\chi(x)=\prod_1^r f_\nu(x)$$

将模 $\mathfrak{M}$ 零化, 因为因子 $f_r(x)$ 将 $\mathfrak{M}$ 零化. 于是有

$$\chi(A)=0. \tag{12.22}$$

特征多项式是 $xE-A$ 的最高阶行列式因子, 因此它除了相差一个常数因子之外等于行列式 $|xE-A|$. 可以立即看出这个常数因子等于 1, 从而

$$\chi(x)=|xE-A|. \tag{12.23}$$

方阵 A 的特征方程 (12.22) 也可以由 (12.23) 通过直接计算导出. 事实上, 有

$$xu_k=\sum u_i\alpha_{ik},$$

由于 x 及其各次幂与 α_{ik} 可交换, 所以由这个方程组中消去所有的 u 就得到

$$\begin{vmatrix} x-\alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ \vdots & \ddots & & \vdots \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & x-\alpha_{nn} \end{vmatrix}\cdot u_j=0,$$

或

$$|xE-A|\cdot u_j=0.$$

这就是说, $\chi(x)=|xE-A|$ 零化所有的 u_j, 从而零化整个模 $\mathfrak{M}$.

根据以上所述, A 的特征多项式的系数在变换 $A\to P^{-1}AP$ 之下不变. 其中最重要的是第一个和末一个系数, 这就是

A 的迹：$-x^{n-1}$ 的系数：

$$S(A)=\sum\alpha_{ii};$$

A 的范数：$(-1)^n x^0$ 的系数：

$$N(A)=|A|.$$

特征函数的根就是上一节中 (作为多项式 $f_\nu(x)$ 的根) 已经引入的特征根 λ_ν. 这一事实给了一个有用的方法来确定这些 λ_ν 和建立前一节中的标准形：先求出

$$\chi(x)=|xE-A|$$

的根 λ_ν, 然后由线性方程组

$$Av_1 = \lambda_\nu v_1$$

求出 v_1(参考 (12.20)). 在有重根 $(\rho > 1)$ 的情形, (12.20) 中其余的 $v_2, \cdots, v_\rho$ 一般很容易求出. 在这一情形下, 可能要把属于同一 λ_ν 的 v_1 换成它们适当的线性组合.

以 λ_ν 为根的方程 $\chi(\lambda) = 0$ 在许多应用中经常出现. 由于它在长期微扰理论中的应用, 这个方程获得了**长期方程**的名称.

12.7　二次型与 Hermite 型

设 K 是一个域, Q 是系数在 K 里的二次型

$$Q(x_1, \cdots, x_n) = \sum_i q_i x_i^2 + \sum_{i<k} q_{ik} x_i x_k. \tag{12.24}$$

如果令 $q_i = q_{ii}$, 并且把 $Q(x_1, \cdots, x_n)$ 写成 $Q(x)$, 那么 (12.24) 可以简化成

$$Q(x) = \sum_{i \leqslant k} q_{ik} x_i x_k.$$

用 y 表示新的不定元序列 $y_1, \cdots, y_n$, 通过计算可得

$$Q(x+y) = Q(x) + Q(y) + B(x, y), \tag{12.25}$$

这里的 $B(x, y)$ 是对称双线性型

$$B(x, y) = \sum b_{ik} x_i y_k, \tag{12.26}$$

其中的系数是

$$\begin{aligned} b_{ii} &= 2q_i, \\ b_{ik} &= b_{ki} = q_{ik} \quad (i < k). \end{aligned}$$

称 $B(x, y)$ 为 $Q(x)$ 的**极型**.

若 x 被线性变换成

$$x_i = \sum \pi_{ij} x'_j \quad (\pi_{ij} \in K), \tag{12.27}$$

则 $Q(x)$ 被变换成新的二次型 $Q'(x)$：

$$Q(x) = Q'(x').$$

这里假定矩阵 $P=(\pi_{ij})$ 是非奇异的. 我们称型 Q 与 Q' 在域 K 里有理等价. 如果矩阵 P 及其逆 P^{-1} 属于环 $\mathfrak{R}\subseteq K$, 则称它们在环 $\mathfrak{R}$ 里等价 (例如当 $\mathfrak{R}=\mathbb{Z}$ 是整数环时, 称为整等价).

如果 y 用与 x 相同的系数 π_{ij} 作变换:

$$y_i=\sum \pi_{ij}y'_j, \tag{12.28}$$

则 $B(x,y)$ 被变换成双线性型 $B'(x',y')$:

$$B(x,y)=B'(x',y').$$

由 (12.25) 可得

$$Q'(x'+y')=Q'(x')+Q'(y')+B'(x',y'). \tag{12.29}$$

所以当 B 是 Q 的极型时, B' 是 Q' 的极型. 因此极型的构造在变量的线性变换下保持不变.

在 (12.25) 中令 $y=x$, 得到

$$4Q(x)=2Q(x)+B(x,x)$$

或

$$2Q(x)=B(x,x). \tag{12.30}$$

如果域的特征不等于 2, 则二次型 $Q(x)$ 可从双线性型 $B(x,x)$ 重新得到

$$Q(x)=\frac{1}{2}B(x,x)=\frac{1}{2}\sum b_{ik}x_ix_k.$$

令 $\dfrac{1}{2}b_{ik}=a_{ik}$, 可以把二次型写成

$$Q(x)=\sum a_{ik}x_ix_k \quad (a_{ik}=a_{ki}). \tag{12.31}$$

双线性型 $B(x,y)$ 的系数 b_{ik} 可以构成一个行列式

$$D=\begin{vmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{vmatrix}=\begin{vmatrix} 2q_1 & q_{12} & \cdots & q_{1n} \\ q_{12} & 2q_2 & \cdots & q_{2n} \\ \vdots & \vdots & & \vdots \\ q_{1n} & q_{2n} & \cdots & 2q_n \end{vmatrix}. \tag{12.32}$$

称 D 为二次型 Q 的行列式. 如果基域的特征不是 2, 我们可以构造半系数 a_{ik} 的行列式 Δ. 这个行列式称为二次型 Q 的判别式. 显然

$$D = 2^n \Delta. \tag{12.33}$$

现在我们探究行列式 D 在线性变换 (12.27) 下的变化情况. 如果把 (12.27) 与 (12.28) 代入 (12.26) 作替换, 即得

$$B'(x', y') = \sum b_{ik} \pi_{ij} \pi_{kl} x'_j x'_l,$$

因此

$$b'_{jl} = \sum b_{ik} \pi_{ij} \pi_{kl}, \tag{12.34}$$

这里是对于重复出现的下标求和. 等式 (12.34) 可以写成矩阵等式

$$B' = P^{\mathrm{T}} B P, \tag{12.35}$$

这里 P^{T} 表示矩阵 $P = (\pi_{ij})$ 的转置.

两边取行列式后得

$$D' = \{\mathrm{Det}(P)\}^2 \cdot D. \tag{12.36}$$

也就是说, 行列式 D 被乘上了变换行列式的平方.

以后我们假设基域的特征不等于 2. 用向量 u 的坐标 c_i 代替变量 x_i, 用向量 v 的坐标 d_i 代替变量 y_i, 并写成

$$f(u, v) = \sum a_{ik} c_i d_k = \frac{1}{2} B(c, d),$$

特别地,

$$f(u, u) = \sum a_{ik} c_i c_k = Q(c).$$

我们现在要通过线性变换将一个二次型 $f(u, u)$ 化成尽可能简单的形式, 先取出一个向量 v_1, 使得 $f(v_1, v_1) \neq 0$. 如果 f 不恒等于零, 这一点是永远可以做到的. v_1 选定之后, 方程 $f(v_1, u) = 0$ 决定空间 R_n 的一个子空间 R_{n-1}, 并且这个子空间不包含 v_1. 如果可能的话, 我们在这个子空间里又取出一个向量 v_2, 使得 $f(v_2, v_2) \neq 0$. 这时方程 $f(v_2, u) = 0$ 和前面的方程一道决定 R_{n-1} 中的一个子空间 R_{n-2}, 并且这个子空间不包含 v_2. 继续这样进行下去, 直到出现这样一个子空间 R_{n-r}, 在这个子空间中对所有的 u 都有 $f(u, u) = 0$, 从而对所有的 u, v 都有 $f(u, v) = 0$[①]. 可能有 $r = n$, 这时 R_{n-r} 就是零子空间. 不然的话, 我们在 R_{n-r} 中

① 在这里用到特征 $\neq 2$ 的假设.

可以任意地选择基元素 $v_{r+1}, \cdots, v_n$. 这时就有

$$\begin{aligned} &f(v_i, v_k) = 0 && (i \neq k), \\ &f(v_i, v_i) = \gamma_i \neq 0 && (i = 1, \cdots, r), \\ &f(v_i, v_i) = 0 && (i = r+1, \cdots, n). \end{aligned}$$

现在我们将每个向量 v 用新的基向量 $v_1, \cdots, v_n$ 表出:

$$v = \sum v_i d_i,$$

这时便有

$$f(v, v) = \sum \sum f(v_i, v_k) d_i d_k = \sum_1^r \gamma_i d_i^2. \tag{12.37}$$

这样, 二次型 f 就如同我们所说的那样, 被化成一个平方和.

R_{n-r} 中的向量 w 具有如下性质: 对所有的 u,

$$f(w, u) = 0,$$

并且这一性质刻画了 R_{n-r} 中的向量 w. 因此, 空间 R_{n-r} 及其维数 $n-r$ 是和 f 不变地相关联着的. 当 K 是有序域 (参见 11.1 节例如实数域的子域) 时 (12.37) 中出现的负的 γ_i 的个数称为 f 的**惯性指数**. 我们证明, 这一惯性指数也是不变的 (Sylvester **惯性定理**).

假设对于另外一组基向量 v_i' 来说, 二次型 f 有表示式

$$f = \sum_1^r \gamma_i' {d'}_i^2,$$

并且设 $\gamma_1, \cdots, \gamma_h$ 是正的, $\gamma_{h+1}, \cdots, \gamma_r$ 是负的; $\gamma_1, \cdots, \gamma_k'$ 是正的, $\gamma_{k+1}', \cdots, \gamma_r'$ 是负的. 如果 $k > h$, 则线性方程组

$$d_1 = 0, \cdots, d_h = 0, \quad d_{k+1}' = 0, \cdots, d_r' = 0$$

定义一个维数大于 $n-r$ 的子空间. 对这个子空间里的一个向量 u 来说, 有 $f(u, u) = \sum\limits_{h+1}^r \gamma_i' d_i^2 \leqslant 0$; 另一方面, 有 $f(u, u) = \sum\limits_1^k \gamma_i' {d'}_i^2 \geqslant 0$. 因此必有 $f(u, u) = 0$, 进而所有的 d_i 和 d_i' 都等于零. 由此可知 u 位于 R_{n-r} 内. 这就是说, 有一个维数大于 $n-r$ 的空间包含在一个维数等于 $n-r$ 的空间之内, 这是不可能的.

如果在 (12.37) 中所有 γ_i 都是正的, 那么当 $r = n$ 时, 称二次型 f 是**正定的**, 而当 $r < n$ 时, 则称 f 是**半定的**. 正定的二次型可以由这样的性质来刻画, 即对于

任意向量 $u \neq 0$, 它所取的值都是正的; 而半定的二次型可以由这样的性质来刻画, 即对于任意向量所取的值并不一定总是正的, 但永远 $\geqslant 0$.

由 (12.37) 立即看出, 将量 $\sqrt{r_i}$ 添加到域 K 上之后, 一个正定的二次型可以化为"单位形式"

$$E(u,u) = \sum d_i^2.$$

和二次型相类似的有 Hermite型. 为了得到 Hermite 型, 我们将有序域 K 中一个负量 α 的平方根 θ, 譬如说, 将 $\theta = \sqrt{-1}$ 添加到 K 上去. 为了区别 K 中的元素和 $K(\theta)$ 中的元素, 我们将 K 中的元素称为"实的", 因为在各种应用中, K 都是实数域, 而 $\theta = \sqrt{-1}$.

每个元素 $c = a + b\theta$ 有一个共轭元素 $\bar{c} = a - b\theta$. 积 $c\bar{c} = a^2 - b^2\theta^2$ 永远是实的并且 $\geqslant 0$, 其中的等号只有当 $c = 0$ 时才成立.

所谓一个 Hermite 型指的是形式如

$$H(u,u) = \sum\sum h_{ik}\bar{c}_i c_k \quad (h_{ik} = \bar{h}_{ki})$$

的一个表达式. 对于任意向量 u, Hermite 型的值都是实的.

如果作

$$\begin{aligned} H(u+\lambda v, u+\lambda v) = &\sum\sum h_{ik}\bar{c}_i c_k + \lambda\sum\sum h_{ik}\bar{c}_i d_k \\ &+ \bar{\lambda}\sum\sum h_{ik}\bar{d}_i c_k + \lambda\bar{\lambda}\sum\sum h_{ik}\bar{d}_i d_k, \end{aligned}$$

那么作为 λ 的系数就得到极式

$$H(u,v) = \sum\sum h_{ik}\bar{c}_i d_k.$$

显然有

$$H(v,u) = \overline{H(u,v)}.$$

对 c_i 作线性变换时, $\bar{c}_i$ 被矩阵为 $\bar{P} = (\bar{\pi}_{ij})$ 的共轭变换所变换, Hermite 型的方阵 H 按照规律

$$H' = P^\dagger H P$$

变换, 这里 $P^\dagger = \bar{P}^{\mathrm{T}}$ 表示共轭转置方阵.

前面关于二次型表成平方和的讨论可以逐字逐句地用于 Hermite 型. 这时将得到标准形

$$H(u,u) = \sum_1^r \gamma_i \bar{c}_i c_i \quad (\gamma_i \text{ 为实元素}). \tag{12.38}$$

和前面一样, Hermite 型 H 称为**正定的**, 如果除了对 $u=0$ 之外, 它的值 $H(u,u)$ 永远是正的, 或者说, $r=n$ 并且 $\gamma_1,\cdots,\gamma_n$ 全都是正数. 添加这些 γ_i 的平方根之后, 每个正定 Hermite 型都可以化为"单位形式"

$$E(u,u)=\sum \bar{c}_i c_i.$$

下面的种种讨论对于 Hermite 型和二次型都同样成立. 我们仅就 Hermite 型来叙述. 只要让在讨论过程中出现的一切量都属于 K, 并且去掉所有的短横, 就可以得出关于二次型的相应的定理.

我们选取一个固定的, n 个变量的正定 Hermite $G(u,u)$ 作为**基本型**, 并且将它的系数方阵 (g_{ik}) 记作 G. 特别, 如果 $G(u,u)$ 是单位形式, 那么 G 就是单位方阵 E. 两个向量 u,v 说是**正交的**, 如果 $G(u,v)=0$. 这时也有 $G(v,u)=0$. 和一个向量 $u\neq 0$ 正交的向量 v 的全体组成一个线性子空间, 称为**与 u 正交的空间**. 如果 G 是正定的, 那么 $G(u,u)\neq 0$, 因此 u 本身不属于与 u 正交的空间 R_{n-1}. 由 n 个相互正交的基向量 $v_1,\cdots,v_n$ 组成的向量系 (如在建立 $G(u,u)$ 的标准形 (12.38) 时所用到的向量系) 称为一个**完备正交系**. 如果 $G(v_j,v_j)=1$, 则称这个正交系为**规范的**.

具有性质

$$G(Au,v)=G(u,Av)\quad (\text{对所有的 } u \text{ 和 } v) \tag{12.39}$$

的线性变换 A 称为 Hermite **对称变换**, 或简称**对称变换**. 把上面的条件具体写出来就是

$$\sum\sum\sum g_{il}\bar{a}_{ij}\bar{c}_j c_l=\sum\sum\sum g_{jk}\bar{c}_j a_{kl}c_l,$$

或

$$\sum_i g_{il}\bar{a}_{ij}=\sum_k g_{ik}a_{kl},$$

或

$$A^{\dagger}G=GA. \tag{12.40}$$

特别, 如果 G 是单位形式, 那么对称条件简单地就是

$$A^{\dagger}=A\quad \text{或}\quad \bar{a}_{ik}=a_{ki}.$$

这就说明了"对称"一词的意义.

使得基本型 $G(u,u)$ 不变, 即满足条件

$$G(Au,Au)=G(u,u)\quad \text{或}\quad A^{\dagger}GA=G \tag{12.41}$$

的线性变换 A 称为酉变换; 在实的情形则称为正交变换. 这时显然也有 $G(Au,Av)=G(u,v)$. 特别, 如果 $G=E$ (在 G 是正定的情形, 我们总可以作这样的假设), 那么这个条件就成为

$$A^{\dagger}A=E \quad \text{或} \quad A^{\dagger}=A^{-1} \quad \text{或} \quad AA^{\dagger}=E.$$

具体书写出来, 就得到下面的“正交性条件”:

$$\sum \bar{a}_{ik}a_{il}=\delta_{kl}=\begin{cases} 0, & \text{如果 } k\neq l, \\ 1, & \text{如果 } k=l, \end{cases}$$

或者与此等价的条件

$$\sum a_{ik}\bar{a}_{jk}=\delta_{ij}.$$

行列式等于 1 的实正交变换称为一个转动.

如果一个对称变换或酉变换 A 将某一非零向量 u 变成它自身的一个倍向量, 即

$$Au=\lambda u, \tag{12.42}$$

也就是说, A 使得由 u 所生成的射线不变, 那么 A 也使得与 u 正交的子空间 R_{n-1} 不变.

证　设 v 属于 R_{n-1}, 因而 $G(u,v)=0$, 于是当 A 是对称变换时有

$$G(u,Av)=G(Au,v)=G(\lambda u,v)=\lambda G(u,v)=0;$$

而当 A 是酉变换时有

$$\begin{aligned} G(u,Av)&=G(AA^{-1}u,Av)=G(A^{-1}u,v) \\ &=G(\lambda^{-1}u,v)=\lambda^{-1}G(u,v)=0. \end{aligned}$$

具有性质 (12.42) 的一个向量 $u\neq 0$ 称为变换 A 的特征向量, 而 λ 则称为相应的特征根.

在 12.6 节中已经看到, 特征根可由“长期方程”

$$\chi(\lambda)=\begin{vmatrix} \lambda-\alpha_{11} & -\alpha_{12}\cdots \\ -\alpha_{21} & \lambda-\alpha_{22}\cdots \\ \vdots & \vdots \end{vmatrix}=0 \tag{12.43}$$

求出, 而相应的特征向量则由等价于 (12.42) 的线性方程组

$$\sum \alpha_{ik}c_k=\lambda c_i \tag{12.44}$$

求出.

现在我们设 K 是一个实闭域 (比方说, 实数域), 从而 $K(\theta)$ 是代数封闭的 (参看 11.5 节). 这时长期方程 (12.43) 在 $K(\theta)$ 中必有一个根 λ_1, 相应于这个根有一个特征向量 e_1. 与 e_1 正交的空间 R_{n-1} 被 A 映入其自身, 并且由于 A 在整个 R_n 中是一个对称变换或酉变换, 它在 R_{n-1} 中也是一个对称变换或酉变换. 因此, 根据同样的论证, 在 R_{n-1} 中有一个特征向量 e_2; R_{n-1} 中与 e_2 正交的空间 R_{n-2} 在 A 之下不变; 如此类推. 最后, 我们可以得出 n 个线性无关的彼此正交的特征向量 $e_1, \cdots, e_n$ 所成的完备正交系

$$Ae_\nu = \lambda_\nu e_\nu.$$

对于新的基 $(e_1, \cdots, e_n)$, 方阵 A 具有对角线形式:

$$A_1 = P^{-1}AP = \begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}. \tag{12.45}$$

如果通过条件 $G(e_\nu, e_\nu) = 1$ 将特征向量规范化, 那么以这些规范化的 e_ν 为基时, G 就等于单位形式 E. 当 K 是实闭域时, 这样的规范化是永远可能的, 因为这时正量 $G(e_\nu, e_\nu)$ 的平方根仍在 K 内. 现在设方阵 A 是对称的, 那么 A_1 也必然是对称的, 因而与 $A_1^\dagger$ 相等. 由此即有

$$\lambda_\nu = \bar{\lambda}_\nu \quad \text{或} \quad \lambda_\nu \in K.$$

方阵 A 或 A_1 的特征多项式是

$$\chi(x) = \prod_1^n (x - \lambda_\nu). \tag{12.46}$$

因此, 对称方阵的长期方程 $\chi(x) = 0$ 的根全是实的.

更进一步, 如果 A 和 G 都是实的, 那么所有的特征向量 e_ν, 作为实线性方程组 (12.44) 的解, 也都是实的. 因此, 一个实对称方阵 A 可以通过实的变换化为对角线形式 (12.45).

任给一个对称变换 A, 有一个 Hermite 型

$$H(u, u) = G(u, Au) = G(Au, u)$$

和它不变地关联着. 这个 Hermite 型的方阵显然是

$$H = GA.$$

反过来, 方阵 A 由这个 Hermite 型唯一确定：

$$A = G^{-1}H.$$

将 A 和 G 化成对角线形式时, $H = GA$ 也同时被化成对角线形式. 经过变换后的 Hermite 型将是

$$H(u,u) = \sum \bar{c}_\nu c_\nu \lambda_\nu.$$

这样我们就证明了：

任何一对 Hermite 型 G 和 H, 如果其中之一, 比方说 G, 是正定的, 可以通过同一变换同时化成

$$\begin{cases} G(u,u) = \sum \bar{c}_\nu c_\nu, \\ H(u,u) = \sum \bar{c}_\nu c_\nu \lambda_\nu \end{cases}$$

的形式, 这里的 λ_ν 是方阵 $A = G^{-1}H$ 的特征根, 或长期方程

$$|\lambda g_{jk} - h_{jk}| = 0$$

的根.

特别, 任何一对实二次型, 如果其中之一是正定的话, 可以通过一个实的变换同时化成平方和[①]：

$$G(u,u) = \sum c_\nu^2,$$

$$H(u,u) = \sum c_\nu^2 \lambda_\nu.$$

习题 12.12 如果 r 个向量 $v_1, \cdots, v_r$ 张成一个 R_r, 那么与所有这些向量正交的向量组成一个 R_{n-r}, 并且整个空间 R_n 是直和 $R_r + R_{n-r}$.

习题 12.13 如果一个对称变换或酉变换 A 使空间 R_r 不变, 那么它也使与 R_r 正交的空间 R_{n-r} 不变.

习题 12.14 任何一组对称变换或酉变换都是完全可约的.

习题 12.15 一个酉变换的行列式 D 的绝对值等于 1, 即 $D\bar{D} = 1$. 一个实正交变换的行列式等于 ± 1.

习题 12.16 一个向量空间到它自身的酉变换组成一个群; 实正交变换同样也组成一个群.

---

① 关于二次型偶分类的一般的处理可以参看 Dickson L E. *Modern algebraic Theories.* Chicago, 1926.

12.8　反对称双线性型

变量 $x_1, \cdots, x_n$ 和 $y_1, \cdots, y_n$ 的一个系数属于域 K 的双线性型

$$f(x,y)=\sum_{i,k} a_{ik}x_iy_k \tag{12.47}$$

叫做反对称的, 如果它具有下面两个性质:

$$f(x,y)=-f(y,x), \tag{12.48}$$

$$f(x,x)=0. \tag{12.49}$$

从系数上来看, 这就意味着

$$a_{ik}=-a_{ki}, \tag{12.50}$$

$$a_{ii}=0. \tag{12.51}$$

如果通过同一线性变换

$$x_i=\sum p_{ij}x'_j,$$
$$y_k=\sum p_{kl}y'_l$$

引入新的变量 x'_j 和 y'_l 来代替 x_i 和 y_k, 则双线性型 $f(x,y)$ 变成一个新的双线性型

$$\begin{aligned} f'(x',y') &= \sum a_{ik}\left(\sum p_{ij}x'_j\right)\left(\sum p_{kl}y'_l\right) \\ &= \sum a'_{jl}x'_jy'_l. \end{aligned}$$

这个双线性型仍是反对称的, 它的系数由

$$a'_{jl}=\sum p_{ij}a_{ik}p_{kl}$$

给出. 采用矩阵记法则是

$$A'=P^{\mathrm{T}}AP. \tag{12.52}$$

由 (12.52) 可得 a_{ik} 的行列式 D 的变换公式

$$D'=D\Delta^2, \tag{12.53}$$

这里 Δ 是变换方阵的行列式.

习题 12.17　证 (12.48) 可由 (12.49) 推出.

我们要适当地选择变换方阵 P, 以便将反对称双线性型 f 化为尽可能简单的标准形. 这一变换要通过几个步骤来实现.

如果 f 恒等于零, 那么 f 不需再作变换便已经具有标准形式

$$f_0 = 0.$$

如果有一个系数不为零, 那么可以假设 $a_{12} \neq 0$. 现在我们把 (12.47) 里含有 x_1 的项全部括出来, 这就是

$$x_1(a_{12}y_2 + \cdots + a_{1n}y_n),$$

这时含有 y_1 的项就是

$$-(a_{12}x_2 + \cdots + a_{1n}x_n)y_1.$$

引入新的变量

$$x'_2 = a_{12}x_2 + \cdots + a_{1n}x_n,$$
$$y'_2 = a_{12}y_2 + \cdots + a_{1n}y_n$$

来代替 x_2 和 y_2, 并且将 f 写成 $x_1, x'_2, x_3, \cdots, x_n$ 和 $y_1, y'_2, y_3, \cdots, y_n$ 的双线性型. 这时含 x_1 和 y_1 的项就简化为

$$x_1y'_2 - x'_2y_1.$$

现在设含有 y'_2 的项为

$$(x_1 + b_3x_3 + \cdots + b_nx_n)y'_2.$$

我们引入新的变量

$$x'_1 = x_1 + b_3x_3 + \cdots + b_nx_n,$$
$$y'_1 = y_1 + b_3y_3 + \cdots + b_ny_n$$

来代替 x_1 和 y_1, 并且将 f 写成 $x'_1, x'_2, x_3, \cdots, x_n$ 和 $y'_1, y'_2, y_3, \cdots, y_n$ 的双线性型. 在这个双线性型里, 含 x'_1, x'_2, y'_1, y'_2 的项只有两项, 就是

$$x'_1y'_2 - x'_2y'_1.$$

所有其余的项都只含 $x_3, \cdots, x_n; y_3, \cdots, y_n$. 如果这些项都为零, 那么我们就得出了标准形

$$f_1 = x'_1y'_2 - x'_2y'_1.$$

不然的话, 我们还可以重复上面的过程, 引进新的变量 x_3', x_4', y_3', y_4' 来代替 x_3, x_4, y_3, y_4, 从而分出一个项

$$x_3'y_4' - x_4'y_3'.$$

继续这样进行下去, 并且最后去掉各个变量符号上的小撇, 就得出标准形

$$f_k = (x_1y_2 - x_2y_1) + \cdots + (x_{2k-1}y_{2k} - x_{2k}y_{2k-1}), \tag{12.54}$$

其中

$$0 \leqslant 2k \leqslant n.$$

在向量 $(c_1, \cdots, c_n)$ 组成的 n 维向量空间中, 方程

$$f(c, y) = 0 \quad \text{对 } y_k \text{ 恒等地成立}$$

或

$$\sum a_{ik}c_i = 0$$

定义一个线性子空间 $\mathfrak{N}$. 如果方阵 A 的秩为 r, 那么这个子空间的维数是 $n - r$. 在 x_i 和 y_k 的可逆线性变换之下, 这个维数显然是型 f 的一个不变量. 因此 r 也是一个不变量.

就标准形 f_k 来计算秩 r, 我们就得到

$$r = 2k. \tag{12.55}$$

由于 r 是一个不变量, 所以原来的型 f 的秩 r 也是一个偶数. 因此有下面的定理:

一个反对称方阵 A 的秩是一个偶数 $2k$. 它等于标准形 (12.54) 中的项数.

如果 n 是奇数, 则 A 的秩必定小于 n, 因而行列式 D 等于零. 反之, 如果 $n = 2m$ 为一偶数, 则存在着行列式 $D \neq 0$ 的反对称双线性型, 例如 f_m 就是. 因此, 一个偶数行的反对称方阵的行列式不恒等于零.

如果当 $i < k$ 时命 a_{ik} 为不相关不定元, 而其余的系数由 (12.50) 和 (12.51) 来定义, 我们就得到一个一般的反对称双线性型. 如果 n 为偶数 $(n = 2m)$, 则根据以上所证, 这个一般反对称型的行列式不恒等于零. 将这个一般型化为标准形, 我们就得到标准形 (12.54), 其中 $k = m$. 变换方阵的系数是不定元 a_{ik} 的有理函数, 而标准形的行列式 D' 等于 1. 因此由 (12.53) 得到

$$D = \Delta^{-2}, \tag{12.56}$$

这里 Δ 是 a_{ik} 的有理函数, 它可以写成两个多项式的商:

$$\Delta = G/H. \tag{12.57}$$

由 (12.56) 和 (12.57) 得出

$$DG^2 = H^2. \tag{12.58}$$

因此 H^2 可以被 G^2 整除, 从而 H 可以被 G 整除：

$$H = GQ.$$

将它代入 (12.57) 和 (12.58) 便得到

$$\Delta = Q^{-1} \tag{12.59}$$

和

$$D = Q^2, \tag{12.60}$$

D 是 a_{ik} 的一个 $n = 2m$ 次齐式, 从而 Q 是 a_{ik} 的一个 m 次齐式. 就 $n = 2$ 和 $n = 4$ 两种情形把这一计算具体作出来, 我们有

$$\begin{aligned} n = 2: &\quad Q = a_{12}, \\ n = 4: &\quad Q = a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23}. \end{aligned}$$

Pfaff 找到了 Q 的一般的公式. 这个公式的一个证明, 可以在逝世后才发表的 Lipschitz 的一封信中找到①.

当 $n = 2m$ 时, 使得标准形 f_m 不变的线性变换所组成的群叫做*辛群*. 关于这种群和正交群以及全线性群的结构, 可参看 Dieudonné J. *Sur les Groupes Classiques*. Paris: Hermann, 1948.

① *Ann.Math.*, 1959, 69: 247.

第 13 章　代　　数

一个环 $\mathfrak{U}$, 如果它同时是某一域 P 上的有限维向量空间, 并且满足条件

$$(\alpha u)v = u(\alpha v) = \alpha(uv) \quad 对\ \alpha \in P,$$

那么就称为域 P 上的一个*结合代数* 或 *超复系*. 如果去掉结合性这一要求, 则所得到的就是 (线性)代数的一般概念. 在非结合代数中, 有两类代数特别值得提出：

(1) *交错代数*. 在这种代数中, 下列受限制的结合律成立：

$$a(ab) = (aa)b,$$

$$b(aa) = (ba)a.$$

交错代数的一个最古老的例子就是 Cayley 的八元数代数. 这方面可以参考 Zorn M. Alternativkörper und quadratische Systeme. *Abh. math. Sem. Univ.. Hamburg*, 1933, 9: 395. 交错代数对于平面几何学的公理研究有着重要意义[①]. 这方面新近的研究可参看 Schafer R D. Structure and representation of nonassociative algebra. *Bull. Amer. math. Soc.,* 1955, 61: 469.

(2) *李* (Lie) *代数*. 在这种代数中, 下列运算规则成立：

$$ab + ba = 0,$$

$$a \cdot bc + b \cdot ca + c \cdot ab = 0.$$

李群的无穷小生成元适合这些规则. 在 Cartan[②]和 Weyl[③] 的奠基性著作中, 结合着李群的理论研究了李代数. 有关新的研究首先可参看：

Witt E. *J. reine u. angew. Math.,* 1937, 177: 152 和 *Abh. math. Sem. Univ.. Hamburg,* 1941, 14: 289.

Freudethal H. *Proc. Akad. Amsterdam,* 1954, A57: 369, 487; 1956, A59: 511; 1958, A61: 379.

---

① Moufang R. Alternativkörper und Satz vom vollständigen Vierseit. *Abh. Math. Sem. Univ.. Hamburg*, 9: 207; 也可以参看 *Math. Ann.*, 110: 416. 此外还可参看 Freudenthal H. Zur ebenen Oktavengeometrie. *Proc. Akad. Amsterdam,* 1953, A56: 195 以及 A57: 218, 363 和 A58: 151.

② Cartem E. Thèse, 1894. 与此有关的是 Freudenthal H. *Proc. Akad. Amsterdam,* 1953, A56.

③ Weyl H. Darstellung halbeinfacher Gruppen durch lineare Transformationen Ⅰ – Ⅲ. *Math. Z.*, 1925, 23: 271 和 1926, 24: 328 和 789 以及 van der Waerden B L. *Math. Z.*, 37: 446.

在本书中, 我们只讨论结合代数. 从现在起, 说到代数, 都指的是域 P 上的一个有限维的结合代数.

13.1　直和与直交

Noether 在她的讲义中曾一再强调模的直和表示与直交表示之间的关系的重要性. 这一观念就像一条红线一样贯穿着她的著作. 现在我们将要对这样一种关系加以说明. 先从乘法群入手, 然后再过渡到加法表示.

一个群 $\mathfrak{G}$ 是子群 $\mathfrak{A}_1, \cdots, \mathfrak{A}_n$ 的直积的意思是：

(1) 每一 $\mathfrak{A}_i$ 都是 $\mathfrak{G}$ 的正规子群;

(2) 乘积 $\mathfrak{A}_1 \cdots \mathfrak{A}_n$ 等于 $\mathfrak{G}$;

(3) 如果 $\mathfrak{B}_i$ 是除 $\mathfrak{A}_i$ 外一切 $\mathfrak{A}_j$ 的乘积, 则

$$\mathfrak{A}_i \cap \mathfrak{B}_i = \mathfrak{E},$$

这里 $\mathfrak{E}$ 仅由单位元素组成.

根据 7.6 节可知, 由 (1)~(3) 可以推出, $\mathfrak{G}$ 中每个元素 g 可以唯一地表成积 $a_1 \cdots a_n (a_i \in \mathfrak{A}_i)$, 并且当 $i \neq j$ 时, $\mathfrak{A}_i$ 中的每个元素与 $\mathfrak{A}_j$ 中每个元素可交换. 其次, 由 (2) 可以推出

$$\mathfrak{A}_i \mathfrak{B}_i = \mathfrak{G}.$$

群 $\mathfrak{B}_i$ 由所有那样的乘积 $a_1 \cdots a_n$ 组成, 其中因子 a_i 等于 e. 由此可以推知, 一切 $\mathfrak{B}_i$ 的交等于 $\mathfrak{E}$, 而一切 $\mathfrak{B}_j (j \neq i)$ 的交等于 $\mathfrak{A}_i$. 这样一来, $\mathfrak{B}_i$ 具有以下三点性质, 这些性质在某种意义下是和 (1)~(3) 互为对偶的：

(1)′ 每个 $\mathfrak{B}_i$ 都是 $\mathfrak{G}$ 的正规子群;

(2)′ 交 $\mathfrak{B}_1 \cap \cdots \cap \mathfrak{B}_n$ 等于 $\mathfrak{E}$;

(3)′ 如果 $\mathfrak{A}_i$ 是除了 $\mathfrak{B}_i$ 之外其余一切 $\mathfrak{B}_j$ 的交, 则

$$\mathfrak{A}_i \mathfrak{B}_i = \mathfrak{G}. \tag{13.1}$$

如果性质 $(1)' \sim (3)'$ 成立, 我们就说单位群 $\mathfrak{E}$ 是 $\mathfrak{B}_1, \cdots, \mathfrak{B}_n$ 的直交. 如果在 $(2)'$ 中将 $\mathfrak{E}$ 换为某一群 $\mathfrak{D}$, 而保持 $(1)'$ 与 $(3)'$ 不变, 则称 $\mathfrak{D}$ 为 $\mathfrak{B}_1, \cdots, \mathfrak{B}_n$ 的直交. 只要作商群 $\mathfrak{G}/\mathfrak{D}$ 和 $\mathfrak{B}_i/\mathfrak{D}$, 就可以将这个较一般的情形归结为 $\mathfrak{D}=\mathfrak{E}$ 的情形.

现在我们从 $(1)' \sim (3)'$ 出发来证明 $(1) \sim (3)$. 如果按 $(3)'$ 中所述方式定义 $\mathfrak{A}_i$, 则由 $(2)'$ 立得

$$\mathfrak{U}_i \cap \mathfrak{B}_i = \mathfrak{E}. \tag{13.2}$$

作为正规子群的交 $\mathfrak{A}_i$ 仍是 $\mathfrak{G}$ 的正规子群. 我们证明, 一切 $\mathfrak{A}_j$ 的乘积等于 $\mathfrak{G}$ 并且除 $\mathfrak{A}_i$ 外其余一切 $\mathfrak{A}_j$ 的乘积等于 $\mathfrak{B}_i$.

设 g 是 $\mathfrak{G}$ 中一个元素. 由 (13.1), (13.2) 可知, $\mathfrak{G}$ 是 $\mathfrak{A}_i$ 和 $\mathfrak{B}_i$ 的乘积, 从而 g 可以唯一地表成

$$g = a_i b_i \quad (a_i \in \mathfrak{A}_i, b_i \in \mathfrak{B}_i)$$

的形式. 其次, $\mathfrak{A}_i$ 中每个元素与 $\mathfrak{B}_i$ 中每个元素可交换, 因而特别与 $\mathfrak{A}_j(j \neq i)$ 中的每个元素可交换. 作乘积

$$g' = a_1 \cdots a_n,$$

则

$$g^{-1}g' = b_i^{-1}a_i^{-1}a_1 \cdots a_n.$$

由于 a_j 的可交换性, 我们可以把这个式子改写成

$$g^{-1}g' = b_i^{-1}a_1 \cdots a_{i-1}a_{i+1} \cdots a_n.$$

右端各个因子都包含在 $\mathfrak{B}_i$ 内. 因此, 对于每个 i 来说, $g^{-1}g'$ 包含在 $\mathfrak{B}_i$ 内. 由 (2)$'$ 知

$$g^{-1}g' = e,$$

亦即 $g' = g$, 因此, $\mathfrak{G}$ 中每个元素可以表成乘积 $a_1 \cdots a_n$. 如果 g 包含在 $\mathfrak{B}_i$ 内, 则因子 $a_i = e$, 于是 $\mathfrak{B}_i$ 中每个元素可以表成乘积

$$a_1 \cdots a_{i-1}a_{i+1} \cdots a_n.$$

这就说明, 一切 $\mathfrak{A}_j$ 的乘积等于 $\mathfrak{G}$, 而除 $\mathfrak{A}_i$ 外其余一切 $\mathfrak{A}_j$ 的乘积等于 $\mathfrak{B}_i$. 这样一来, $\mathfrak{A}_i$ 就具有性质 (1)~(3).

根据第一同构定理, 由 (13.1) 和 (13.2) 可得

$$\mathfrak{G}/\mathfrak{B}_i \cong \mathfrak{A}_i.$$

如果采取加法表示, 则以上所证可改述如下：

若一个模 $\mathfrak{G}$ 是子模 $\mathfrak{A}_1, \cdots, \mathfrak{A}_n$ 的直和, 而 $\mathfrak{B}_i$ 是除 $\mathfrak{A}_i$ 外一切 $\mathfrak{A}_j$ 的和, 则 $\mathfrak{B}_1, \cdots, \mathfrak{B}_n$ 的直交是 $\{0\}$; 除 $\mathfrak{B}_i$ 外其余一切 $\mathfrak{B}_j$ 的交就是 $\mathfrak{A}_i$. 反之亦然. 更进一步, 我们有 $\mathfrak{G}/\mathfrak{B}_i \cong \mathfrak{A}_i$.

上面一切论断对于带算子的群来说也成立. 在环论的应用中, $\mathfrak{G}$ 是一个以 $\mathfrak{G}$ 自身作为它的左或右算子区的环. 这时模 $\mathfrak{A}_i$ 和 $\mathfrak{B}_i$ 就是 $\mathfrak{G}$ 中的左或右理想. 这样一来, 我们所讨论的就是一个环 $\mathfrak{G}$ 被表成它的左或右理想 $\mathfrak{A}_i$ 的直和, 以及零理想

相应地被表成左或右理想 $\mathfrak{B}_i$ 的直交的问题. 群论的语言仍可继续采用, 因为在这一理论中, 每一个环原则上总可以看作一个加法群, 而以其自身作为算子区.

如果一切 $\mathfrak{A}_i$(从而一切 $\mathfrak{B}_i$) 都是双边理想, 则 $\mathfrak{A}_i\mathfrak{A}_j$ 既包含在 $\mathfrak{A}_i$ 内也包含在 $\mathfrak{A}_j$ 内. 然而当 $i \neq j$ 时, $\mathfrak{A}_i \cap \mathfrak{A}_j$ 等于零理想, 从而 $\mathfrak{A}_i\mathfrak{A}_j = \{0\}$. 由此即得下面的结论:

如果环 $\mathfrak{G}$ 是双边理想 $\mathfrak{A}_i$ 的直和:

$$\mathfrak{G} = \mathfrak{A}_1 + \cdots + \mathfrak{A}_n, \tag{13.3}$$

则 $\mathfrak{A}_i$ 都是互相零化的环:

$$\mathfrak{A}_i\mathfrak{A}_j = \{0\} \quad \text{对} \quad i \neq j. \tag{13.4}$$

反之, 如果将 $\mathfrak{G}$ 看成加法群时, 它是互相零化的环 $\mathfrak{A}_i$ 的直和, 则这些 $\mathfrak{A}_i$ 都是 $\mathfrak{G}$ 的双边理想. 证明是显易的. 在这样的情况下, 我们就说环 $\mathfrak{G}$ (或者特别地代数 $\mathfrak{G}$) 是*环 (或代数) $\mathfrak{A}_i$ 的直和*.

如果 (13.3) 和 (13.4) 成立, 那么环 $\mathfrak{G}$ 的结构可以简单地由环 $\mathfrak{A}_i$ 的结构来决定. 事实上, 如果 g 和 h 是两个环元素, 那么当我们依照 (13.3) 将它们表成和

$$g = g_1 + \cdots + g_n,$$

$$h = h_1 + \cdots + h_n$$

时, 则

$$g + h = (g_1 + h_1) + \cdots + (g_n + h_n),$$
$$gh = g_1h_1 + \cdots + g_nh_n.$$

这就是说, 两个元素相加或相乘时, 只要把它们的各个分量分别地相加或相乘即可.

习题 13.1 如果一个有单位元的环是左理想的直和:

$$\mathfrak{G} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n, \tag{13.5}$$

并且单位元的分解由

$$e = e_1 + \cdots + e_n \tag{13.6}$$

给出, 则 $\mathfrak{l}_i = \mathfrak{G}e_i$, 并且有

$$e_i^2 = e_i, \tag{13.7}$$

$$e_ie_j = 0 \quad (i \neq j). \tag{13.8}$$

反之, 如果 (13.6)~(13.8) 成立, 并且令

$$\mathfrak{l}_i = \mathfrak{G}e_i, \tag{13.9}$$

则 $\mathfrak{G}$ 是左理想 $\mathfrak{l}_i$ 的直和. 同样, 如果定义

$$\mathfrak{r}_i = e_i\mathfrak{G}, \tag{13.10}$$

则 $\mathfrak{G}$ 是右理想 $\mathfrak{r}_i$ 的直和.

13.2 代 数 举 例

例 1 代数的一个重要例子, 就是系数属于 P 的一切 n 阶方阵所组成的全阵环 P_n. 这个代数的秩等于 n^2. 我们可以取方阵 C_{ik} 作为基元素, 其中第 i 行和第 k 列的交点处是 1, 而其余的位置都是零. 每一个系数是 α_{ik} 的矩阵 A 可以表成和

$$\sum C_{ik}\alpha_{ik},$$

这里对一切 i 和 k 从 1 到 n 求和. 基元素相乘的规则是

$$C_{hi}C_{jk} = 0 \quad (i \neq j),$$

$$C_{hi}C_{ik} = C_{hk}.$$

例 2 四元数代数. 设 $\mathfrak{A}$ 是一个四维向量空间, 基元素为 e, j, k, l. 令 e 代表单位元, 从而有 $e^2 = e, ej = j$, 等等. 其次, 令

$$j^2 = -e\alpha, \quad k^2 = -e\beta,$$

这里 α 和 β 是 P 的任意元素, 并且令

$$jk = -kj = l.$$

这样一来就有

$$l^2 = jkjk = -jjkk = -e\alpha\beta,$$

$$jl = jjk = -e\alpha k = -k\alpha,$$

$$lj = -kjj = ke\alpha = k\alpha,$$

$$kl = -kkj = e\beta j = j\beta,$$

$$lk = jkk = -je\beta = -j\beta.$$

这样定义的代数 $\mathfrak{A}$ 称为一个广义四元数代数. 它的元素是

$$x = ex_0 + jx_1 + kx_2 + lx_3 \quad (x_0, x_1, x_2, x_3 \text{ 属于 } P).$$

元素 ex_0 显然可以和 x_0 等同起来, 从而 P 就被嵌入 $\mathfrak{A}$ 内.

元素 x 的范数定义为

$$\begin{aligned} N(x) = x\bar{x} &= (ex_0 + jx_1 + kx_2 + lx_3)(ex_0 - jx_1 - kx_2 - lx_3) \\ &= x_0^2 + \alpha x_1^2 + \beta x_2^2 + \alpha\beta x_3^2. \end{aligned}$$

如果这个二次型能表示零 (就是说, 对于 x_i 的一组不全为零的值二次型取值零), 那么当 $x \neq 0$ 时, $x\bar{x}$ 仍有可能为零, 从而 $\mathfrak{A}$ 有零因子. 如果这个二次型不能表示零, 那么每一个 $x \neq 0$ 都有一个逆元素

$$x^{-1} = \bar{x}(x_0^2 + \alpha x_1^2 + \beta x_2^2 + \alpha\beta x_3^2)^{-1},$$

这时 $\mathfrak{A}$ 就是一个体.

如果将 $\mathfrak{A}$ 看成一个双模, 以 $\mathfrak{A}$ 本身作为左算子区, 而以 $\Sigma = P(j)$ 作为右算子区, 那么就可以得出 $\mathfrak{A}$ 的一个方阵表示. 假设 $-\alpha$ 在 P 中没有平方根, 则

$$\Sigma = P(j) = P(\sqrt{-\alpha})$$

是一个域, $\mathfrak{A}$ 是这个域上的一个二维向量空间, 我们可以取 e 和 $-k$ 作为基元素. 于是向量 x 可以写成

$$x = e(x_0 + jx_1) + (-k)(-x_2 + jx_3). \tag{13.11}$$

用任意元素 y 去左乘向量 x, 就得到向量空间 $\mathfrak{A}$ 的一个线性变换 Y. 这个线性变换可由一个方阵来表示. 我们把这个方阵仍记作 Y. 用 y 左乘基元素 e 和 $-k$, 并且将结果仍表成 (13.11) 的形式, 就得出方阵 Y 的两个列. 特别地, 如果取 y 等于 j, k 或 l, 就得出方阵

$$J = \begin{pmatrix} j & 0 \\ 0 & -j \end{pmatrix}, \quad K = \begin{pmatrix} 0 & \beta \\ -1 & 0 \end{pmatrix}, \quad L = \begin{pmatrix} 0 & j\beta \\ j & 0 \end{pmatrix}. \tag{13.12}$$

选取 $\alpha = \beta = 1$, 我们得到 Hamilton 四元数：

$$x = ex_0 + jx_1 + kx_2 + lx_3,$$

其运算规则是

$$j^2 = k^2 = l^2 = -1,$$

$$jk = l, \qquad kj = -l,$$

$$kl = j, \qquad lk = -j,$$

$$lj = k, \qquad jl = -k.$$

如果 P 是实数域, 那么在矩阵表示中可以把 j 换成虚数单位 i, 于是得到

$$J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad L = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

例 3 如果取一个有限群中的元素 $u_1, \cdots, u_n$ 作为一个代数的基元素, 就得到这个有限群的*群环*. 结合律是自然成立的.

例 4 Grassmann*外乘法*. 我们从一个向量空间

$$\mathfrak{M} = u_1 P + \cdots + u_n P$$

出发, 提出这样一个问题, 即设法定义一种满足结合律的乘法, 并且使得

$$uu = 0 \quad 和 \quad uv + vu = 0 \tag{13.13}$$

成立. 为此目的, 我们首先纯形式地作出基向量 u_i 在自然顺序之下的乘积

$$u_{ijk\cdots} = u_i u_j u_k \cdots \quad (i < j < k < \cdots),$$

其中也包括空的乘积 e. 我们取这 2^n 个乘积作为一个向量空间 $\mathfrak{A}$ 的基元素. 这样一来, $\mathfrak{A}$ 中的元素就是一切可能的和

$$e\alpha + \sum_i u_i \alpha_i + \sum_{i<j} u_{ij} \alpha_{ij} + \cdots + u_{12\cdots n} \alpha_{12\cdots n}. \tag{13.14}$$

现在我们按下述方式定义任意乘积

$$u_{abc\cdots} = u_a u_b u_c \cdots. \tag{13.15}$$

如果在 (13.15) 中某两个足数相同, 则命 $u_{abc\cdots} = 0$. 如果所有的足数都不相同, 那么就通过一个置换将它们改变成自然顺序 $ijk\cdots$, 并且命

$$u_{abc\cdots} = \varepsilon u_{ijk\cdots},$$

这里对于偶置换取 $\varepsilon = +1$, 对于奇置换取 $\varepsilon = -1$.

最后, 两个基元素的乘积由

$$u_{ijk\cdots} u_{pqr\cdots} = u_{ikj\cdots pqr\cdots} \tag{13.16}$$

来定义. 形如 (13.14) 的两个和相乘时, 就将各项按 (13.16) 分别相乘, 再将所得结果相加. 根据这一定义, 乘积 $u_a u_b \cdots$ 的确像 (13.15) 中所要求的那样, 等于 $u_{ab\cdots}$. 规律 (13.13) 显然成立. 乘法的结合律是很容易证明的.

形如 (13.14) 的和带有这样的乘法定义构成向量空间 $\mathfrak{M}$ 的 Grassmann代数 $\mathfrak{A}$, 这个乘法则称为外乘法. 向量空间 $\mathfrak{M}$ 是嵌在 $\mathfrak{A}$ 内的. 人们经常用 $a \wedge b$ 作为外乘积的记号.

代数 $\mathfrak{A}$ 还有一个与上面的定义等价的定义. 首先由 $\mathfrak{M}$ 作张量环, 它是由一切有限和

$$e\beta + \sum u_i\beta_i + \sum u_{ij}\beta_{ij} + \sum u_{ijk}\beta_{ijk} + \cdots \tag{13.17}$$

组成的, 其中足数 $i, j, \cdots$ 不受任何限制. 两个这样的和只有在它们的一切对应的系数相等时才算作相等的. 这种和如何相加是显然的. 乘法由 (13.16) 来定义.

不难看出, 张量环中的加法与乘法不依赖于基向量的选取.

现在我们在张量环 $\mathfrak{T}$ 中作双边理想 $\mathfrak{J}$, 它由乘积 uu 生成, 其中 u 遍历 $\mathfrak{M}$ 中一切向量. 向量

$$(u+v)(u+v) - uu - vv = uv + vu$$

也属于 $\mathfrak{J}$.

如果对于每个和 (13.17), 使代数 $\mathfrak{A}$ 中的同样一个和与它对应, 就得到 $\mathfrak{T}$ 到 $\mathfrak{A}$ 上的一个同态映射. 在这个同态之下, $\mathfrak{J}$ 中的元素被映成零. 反之, 如果在上述映射之下, 和 (13.17) 被映成零, 那么这个和必定属于 $\mathfrak{J}$. 事实上, 我们可以把 (13.17) 先写成

$$e\beta + \sum u_i\beta_i + \sum u_iu_j\beta_{ij} + \sum u_iu_ju_k\beta_{ijk} + \cdots \tag{13.18}$$

的形式, 然后把 $\mathfrak{J}$ 中的一些适当的元素加到它上面, 将它变成标准形

$$e\alpha + \sum_i u_i\alpha_i + \sum_{i<j} u_iu_j\alpha_{ij} + \sum_{i<j<h} u_iu_ju_k\alpha_{ijk} + \cdots .$$

对于这样一个和有 $\mathfrak{A}$ 中具有同样系数 $\alpha, \alpha_i, \alpha_{ij}, \cdots$ 的元素 (13.14) 与它对应. 如果这个元素为零, 那么所有这些系数都等于零, 从而和 (13.18) 属于 $\mathfrak{J}$. 因此, $\mathfrak{J}$ 恰为环同态 $\mathfrak{T} \to \mathfrak{A}$ 的核, 并且

$$\mathfrak{A} \cong \mathfrak{T}/\mathfrak{J}. \tag{13.19}$$

在 (13.19) 的右端 $\mathfrak{T}$ 和 $\mathfrak{J}$ 都与基元素 $(u_1, \cdots, u_n)$ 的选择无关. 因此, 代数 $\mathfrak{A}$ 在同构意义下与基的选择无关. 如果就直接定义 $\mathfrak{A}$ 为 $\mathfrak{T}/\mathfrak{J}$, 就得到 Grassmann 代数 $\mathfrak{A}$ 的一个不变定义.

例 5 Clifford代数. 这一代数可以完全类似于 Grassmann 代数那样来定义. 设 $Q(x)$ 是 $x_1, \cdots, x_n$ 的一个二次型, 系数取自 P:

$$Q(x_1, \cdots, x_n) = \sum_i q_i x_i^2 + \sum_{i<j} q_{ij} x_i x_j.$$

于是, 对于 $\mathfrak{M}$ 中每一个向量 $u = \sum u_i \gamma_i$, 二次型的值

$$Q(u) = Q(\gamma_1, \cdots, \gamma_n)$$

均有定义. 此外, 对于任意两个向量 u 和 v, 对称双线性型

$$B(u, v) = Q(u+v) - Q(u) - Q(v)$$

有定义. 特别有

$$Q(u_i) = q_i,$$

$$B(u_i, u_j) = B(u_j, u_i) = q_{ij} \quad (i < j).$$

我们现在将定义向量的一个乘法, 使得

$$uu = Q(u), \tag{13.20}$$

$$uv + vu = B(u, v) \tag{13.21}$$

成立. 这里 (13.21) 是 (13.20) 的一个推论：

$$\begin{aligned} uv + vu &= (u+v)(u+v) - uu - vv \\ &= Q(u+v) - Q(u) - Q(v) = B(u, v). \end{aligned}$$

特别地, 有

$$u_i u_i = q_i, \tag{13.22}$$

$$u_i u_j + u_j u_i = q_{ij} \quad (i < j). \tag{13.23}$$

我们仍作出一个 2^n 维向量空间, 它由和

$$e\alpha + \sum_i u_i \alpha_i + \sum_{i<j} u_{ij} \alpha_{ij} + \cdots + u_{12\cdots n} \alpha_{12\cdots n} \tag{13.24}$$

组成.

现在定义任意乘积

$$u_a u_b u_c \cdots = u_{abc\cdots}. \tag{13.25}$$

当足数 $a, b, c, \cdots$ 互异, 并且按自然顺序排列时, 则 $u_{abc\cdots}$ 就是我们的 2^n 个基向量之一. 在一切其他情况下, 我们利用规则 (13.22) 和 (13.23) 作乘积 $u_a u_b u_c \cdots$ 的

变形. 例如, 若 bc 是第一对相继出现但不按自然顺序排列的足数, 我们就把乘积 (13.25) 改写为 $u_a(u_b u_c)\cdots$, 并且依照 (13.22) 和 (13.23) 作 $u_b u_c$ 的变形：

$$u_b u_b = q_b \quad (c = b),$$
$$u_b u_c = -u_c u_b + q_{cb} \quad (c < b).$$

因子 q_b 和 q_{cb} 都写在乘积的前面. 于是

$$u_a(u_b u_b)\cdots = q_b u_a \cdots ,$$
$$u_a(u_b u_c)\cdots = -u_a u_c u_b + q_{cb} u_a \cdots .$$

经过变形之后, 或者乘积中的因子减少两个, 或者反序数减少一个. 如此继续下去, 最后一定得出形如 (13.24) 的表示式.

这样定义了乘积之后, 我们又可以利用 (13.16) 来定义两个基元素的乘积, 并且证明乘法的结合律. 这样一来, 就完全定义了属于二次型 $Q(x)$ 的 Clifford 代数 $\mathfrak{C}$. 如果二次型 Q 恒等于零, 则 Clifford 代数就转化为 Grassmann 代数.

如果在 (13.24) 中只限于取带偶数个足数的项 $u_{ij\cdots}$：

$$e\alpha + \sum_{i<j} u_{ij}\alpha_{ij} + \sum_{i<j<k<l} u_{ijkl} a_{ijkl} + \cdots ,$$

我们就得到一个子代数, 称为第二 Clifford 代数 $\mathfrak{C}_+$.

如果在张量环 $\mathfrak{T}$ 中取由一切表达式

$$uu - Q(u)$$

所生成的双边理想 $\mathfrak{I}$, 并且作同余类环 $\mathfrak{T}/\mathfrak{I}$, 我们就得到 Clifford 代数 $\mathfrak{C}$ 的一个不变定义. Chevalley [①] 从这一定义出发, 建立了任意域上 Clifford 代数的理论. 关于不变定义与上述定义相同的简单证明可在 van der Waerden 的文章 *Proc. Kon. Ned. Akad. Amsterdam*, 69: 78 里找到.

Brauer 和 Weyl 在 *Amer. J. Math.*, 57: 245 中曾利用第二 Clifford 代数将正交变换 (即使得二次型 Q 不变的、行列式为 1 的线性变换 T) 表成

$$Tu = \mathfrak{s}u\mathfrak{s}^{-1}$$

的形式, 这里 u 遍历向量空间 $\mathfrak{M}$, 而 $\mathfrak{s}$ 是 $\mathfrak{G}_+$ 中使得 $\mathfrak{M}$ 不变的元素：

$$\mathfrak{s}\mathfrak{M}\mathfrak{s}^{-1} = \mathfrak{M}.$$

① Chevalley C. *The algebraic theory of spinors.* Columbia University Press, 1954.

这里必须假定 P 的特征不是 2, 而二次型 Q 是非奇异的. 特征为 2 的情况较为复杂 (参看 Chevalley 的书, 定理 II, 3.3).

习题 13.2 如果二元二次型

$$Q(x_1, x_2) = q_1 x_1^2 + q_{12} x_1 x_2 + q_2 x_2^2$$

在基域 P 内不能分解成一次因子, 则属于 Q 的第二 Clifford 代数就是使得这个二次型能够分解的二次扩域.

习题 13.3 三元二次型

$$Q(x_1, x_2, x_3) = q_1 x_1^2 + q_2 x_2^2 + q_3 x_3^2$$

的第二 Clifford 代数就是广义四元数代数.

13.3 积 与 叉 积

向量空间的积

设 $\mathfrak{A}$ 和 $\mathfrak{B}$ 是域 P 上的两个有限维向量空间:

$$\mathfrak{A} = u_1 P + \cdots + u_m P,$$

$$\mathfrak{B} = v_1 P + \cdots + v_n P.$$

我们要定义积 $\mathfrak{A} \times \mathfrak{B}$. 为此目的, 我们作出 mn 个基向量 w_{ik}, 其中 i 从 1 变到 m, k 从 1 变到 n, 及积空间

$$\mathfrak{C} = \sum_{i,k} w_{ik} P,$$

并对 $\mathfrak{A}$ 中每个 u 和 $\mathfrak{B}$ 中每个 v 定义一个乘积

$$uv = \left(\sum u_i \alpha_i\right)\left(\sum v_k \beta_k\right) = \sum_{i,k} \omega_{ik} \alpha_i \beta_k.$$

特别地, 有

$$u_i v_k = w_{ik}.$$

这样一来, $\mathfrak{C}$ 中的一切元素都是下面这种形状的表达式

$$w = \sum_{i,k} u_i v_k \gamma_{ik} = \sum_{i,k} w_{ik} \gamma_{ik}. \tag{13.26}$$

我们把这样的表达式称为**二阶张量**, 而把积空间 $\mathfrak{C}$ 称为**张量空间**.

(13.26) 也可以改写成

$$w = \sum_i u_i b_i, \tag{13.27}$$

其中 b_i 为 $\mathfrak{B}$ 中任意元素. 这样一来, 空间 $\mathfrak{C}$ 就是子空间 $u_i\mathfrak{B}$ 的直和:

$$\mathfrak{C} = u_1\mathfrak{B} + \cdots + u_m\mathfrak{B}. \tag{13.28}$$

公式 (13.28) 表明, 模 $\mathfrak{C}$ 与 $\mathfrak{B}$ 中基向量的选择无关. 我们可以把 $\mathfrak{C}$ 中的元素直接写成 (13.27) 的形式, 然后定义它们的相加以及这些元素与 P 中元素相乘的运算, 而不必事先在 $\mathfrak{B}$ 中引入一个基.

同样, (13.26) 也可写成

$$w = \sum a_k v_k. \tag{13.29}$$

这样一来, 就有

$$\mathfrak{C} = \mathfrak{A}v_1 + \cdots + \mathfrak{A}v_n, \tag{13.30}$$

从这里立即看出, 积空间 $\mathfrak{C}$ 也与 $\mathfrak{A}$ 的基的选择无关.

即使在 $\mathfrak{A}$ 为有限维向量空间, 而 $\mathfrak{B}$ 为任意 P 模的情形, 也可以利用 (13.28) 来构造模 $\mathfrak{C} = \mathfrak{A} \times \mathfrak{B}$. 同样, 在 $\mathfrak{A}$ 为任意 P 模, 而 $\mathfrak{B}$ 为有限维向量空间的情形下, 可利用 (13.30) 来构造 $\mathfrak{C}$.

积模 $\mathfrak{A} \times \mathfrak{B}$ 也可以不利用基来定义. 这样一个不变定义即使在 P 为一个具有单位元的交换环, 而 $\mathfrak{A}$ 和 $\mathfrak{B}$ 为任意 P 模的情形也是有意义的, 只要 P 中的单位元是 $\mathfrak{A}$ 和 $\mathfrak{B}$ 的单位算子就行了. 由于在今后我们只要用到 P 为一域, 而 $\mathfrak{U}$ 或 $\mathfrak{B}$ 是有限维的情况, 因此我们满足于本节开头处所给的定义. 关于一般的情况, 建议读者去参看 Bourbaki N 的*Algèbre multilinéaire*(*Eléments de Mathématique, Livre* II, *Chap.*III; *Actualités Scient.*, 1104).

用完全相同的方法可以构造 3 个或更多向量空间的积空间

$$\mathfrak{A} \times \mathfrak{B} \times \mathfrak{C} = (\mathfrak{A} \times \mathfrak{B}) \times \mathfrak{C} = \mathfrak{A} \times (\mathfrak{B} \times \mathfrak{C}). \tag{13.31}$$

代数的积

如果 $\mathfrak{A}$ 和 $\mathfrak{B}$ 是 P 上的代数, 那么只要按如下方式来定义基元素 w_{ik} 的乘积:

$$\omega_{ik} w_{jl} = (u_i v_k)(u_j v_l) = (u_i u_j)(v_k v_l), \tag{13.32}$$

就可以把模 $\mathfrak{C} = \mathfrak{A} \times \mathfrak{B}$ 转变成一个代数.

如果将 $\mathfrak{C}$ 中的元素表成 (13.27) 的形式, 并用

$$\left(\sum u_i b_i\right)\left(\sum u_j b'_j\right) = \sum_{i,j} u_i u_j b_i b'_j$$

来定义它们的乘积, 那么就可以使得乘法的定义与 $\mathfrak{B}$ 中基的选择无关. 用文字表达出来, 这就是说: 在作 $\mathfrak{C}$ 中元素的乘积的时候, 可以将 $\mathfrak{A}$ 中的基元素按它们在 $\mathfrak{A}$ 中相乘的规则相乘, 但同时取 $\mathfrak{B}$ 代替 P 来作为系数环. 这样得到的代数用记号 $\mathfrak{A}_{\mathfrak{B}}$ 来表示. 当 $\mathfrak{B}$ 为一个将 P 包含在自己的中心之内的任意环时, 这一记法亦能适用. 因此, $\mathfrak{A}_{\mathfrak{B}}$ 就是那样一个一般的代数, 它和 $\mathfrak{A}$ 有相同的基元素, 但以 $\mathfrak{B}$ 作系数环.

显然有

$$\mathfrak{A} \times \mathfrak{B} \cong \mathfrak{B} \times \mathfrak{A}.$$

事实上, 只要将 $u_i v_k$ 映射成 $v_k u_i$, 并将这一映射线性地开拓到一切和 (13.26) 之上去, 就可以建立起 $\mathfrak{A} \times \mathfrak{B}$ 和 $\mathfrak{B} \times \mathfrak{A}$ 之间的一个同构.

对于全阵环来说, 有两个乘积关系是值得注意的. 命 $\mathfrak{A}_r$ 表示系数属于 $\mathfrak{A}$ 的一切 r 阶方阵所组成的环. 这时我们有

$$\mathfrak{A} \times P_r \cong \mathfrak{A}_r, \tag{13.33}$$

$$P_r \times P_s = P_{rs}. \tag{13.34}$$

为了证明 (13.33), 只需注意在 13.2 节中所定义的方阵 C_{ik} 构成 P_r 的一个基. 为了作出 $P_r \times \mathfrak{A}$, 我们仍取这些元素作为基元素, 但以 $\mathfrak{A}$ 作为系数环, 而这样所得到的就是 $\mathfrak{A}_r$.

(13.34) 可以证明如下. 设 P_r 由 r^2 个基元素 C'_{ik} 张成, P_s 由 s^2 个基元素 C''_{jl} 张成, 则 $P_r \times P_s$ 由 $r^2 s^2$ 个基元素

$$C_{ij,kl} = C'_{ik} C''_{jl}$$

张成. 这些基元素满足关系式:

$$C_{ij,kl} C_{mn,pq} = \begin{cases} 0, & \text{如果 } k \neq m \text{ 或 } l \neq n, \\ C_{ij,pq}, & \text{如果 } k = m, l = n. \end{cases}$$

现在用足数 J 来代表 rs 个足数对 ij, 则 J 由 1 变到 rs, 这样一来就有

$$C_{JK} C_{LM} = \begin{cases} 0, & \text{对 } K \neq L, \\ C_{JM}, & \text{对 } K = L. \end{cases}$$

从这里就可看出 $P_r \times P_s$ 与 P_{rs} 的同构性.

叉积

设 Σ 是 P 的一个可分正规有限扩域. Σ 的 Galois 群 $\mathfrak{G}$(8.1 节) 由 Σ 的那样一些自同构 S_i 组成, 它们使得 P 中一切元素不变. 我们不假定读者有整个 Galois 理论的知识, 仅假定读者知道 8.1 节中的内容, 特别是那样一个事实, 即群 $\mathfrak{G}$ 的阶等于域的次数 $n=(\Sigma:P)$.

我们用 β^S 表示将自同构 S 作用于 Σ 中元素 β 所得到的那个元素. S 和 T 的积 (先作 S, 后作 T) 这时将记作 ST. 这样一来, 就有

$$\beta^{ST}=(\beta^S)^T$$

由 Noether 所引入的域 Σ 和它的 Galois 群 $\mathfrak{G}$ 的**叉积**是这样定义的. 对 $\mathfrak{G}$ 中每个元素 S_i, 我们使一个基向量 u_i 与之相当, 从而作出一个向量空间：

$$\mathfrak{A}=u_1\Sigma+\cdots+u_n\Sigma.$$

去掉 S_i 的足数, 把它简写成 S, 相应的基向量 u_i 改写成 u_S. 这样一来, 向量空间 $\mathfrak{A}$ 由一切和

$$\sum_i u_i\beta_i=\sum_S u_S\beta_S \tag{13.35}$$

组成.

现在用公式

$$\beta u_S=u_S\beta^S \tag{13.36}$$

来定义乘积 βu_S, 而用

$$u_Su_T=u_{ST}\delta_{S,T} \tag{13.37}$$

定义乘积 u_Su_T, 其中因子 $\delta_{S,T}$ 暂设为 Σ 中一个不等于零的任意元素.

利用 (13.36) 和 (13.37) 可以将任意两个形如 (13.35) 的和相乘. 为此只需将各个项分别相乘：

$$u_S\beta\cdot u_T\gamma=u_Su_T\beta^T\gamma=u_{ST}\delta_{S,T}\beta^T\gamma,$$

并将所得乘积相加即可.

为了使得由因子系 $\delta_{S,T}$ 所定义的乘法满足结合律, $\delta_{S,T}$ 必须满足如下的结合性条件：

$$\delta_{S,TR}\delta_{T,R}=\delta_{ST,R}(\delta_{S,T})^R. \tag{13.38}$$

在基向量 u_S 以及因子 $\delta_{S,T}$ 的选择上是存在着一定的任意性的. 事实上, 我们可以将 u_S 换成

$$v_S=u_S\gamma_S\quad(\gamma_S\neq 0 \text{ 属于 } \Sigma), \tag{13.39}$$

和这一新基相应的因子系将是

$$\varepsilon_{S,T} = \frac{\gamma_S^T \gamma_T}{\gamma_{ST}} \delta_{S,T}. \tag{13.40}$$

由 (13.40) 这样一个关系式联系着的两个因子系 $\delta_{S,T}$ 和 $\varepsilon_{S,T}$ 称为相伴因子系. 相伴因子系定义同一代数 $\mathfrak{A}$.

设 $\mathfrak{G}$ 的单位元为 E. 我们总可以将 u_E 乘上一个适当的因子 γ_E, 使得

$$u_E u_E = u_E$$

成立, 因而有 $\delta_{E,E} = 1$. 这时由结合律

$$(u_E u_E) u_R = u_E (u_E u_R),$$

$$u_S (u_E u_E) = (u_S u_E) u_E$$

可以推知 u_E 是 $\mathfrak{A}$ 中的单位元, 因而可以把乘积 $u_E \beta$ 和 Σ 中的元素 β 等同起来.

怎样的元素 $c = \sum u_S \gamma_S$ 和 Σ 中一切元素 β 可交换? 条件 $c\beta = \beta c$ 给出

$$\sum u_S \beta^S \gamma_S = \sum u_S \gamma_S \beta,$$

因而由 u_S 的线性无关性有

$$(\beta^S - \beta)\gamma_S = 0.$$

对 $S = E$ 这一条件自然满足. 当 $S \neq E$ 时, 在 Σ 中总可找到一个元素 β, 使 $\beta^S \neq \beta$, 从而必有 $\gamma_S = 0$. 因此

$$c = u_E \gamma_E = \gamma_E$$

是 Σ 中的一个元素.

由此即得下面的结论：Σ是代数 $\mathfrak{A}$ 中的一个极大交换子环.

现在我们决定环 $\mathfrak{A}$ 的中心, 即 $\mathfrak{A}$ 中与 $\mathfrak{A}$ 的一切元素可交换的元素 c 的集合：

$$ac = ca, \quad 对一切 \ a.$$

如果 c 是一个中心元素, 则 c 首先必须和 Σ 中一切元素可交换, 因而包含在 Σ 之内. 因此可以假定 $c = \gamma$. 进一步, 根据 (13.36), 为了使得 γ 与一切 u_S 可交换, γ 必须在一切自同构 S 之下保持不变. 根据 8.1 节中最后一个定理, 这一情况当且仅当 γ 属于基域 P 时才能成立. 因此

$\mathfrak{A}$ 的中心是 P.

域 P 上的代数, 其中心恰为 P 者, 称为 P 上的中心代数. 早些时候曾经使用过 "正规" 代数这一名称, 可是这个名词的各种不同意义实在是太多了.

作为第二步, 我们证明如下的定理:

定理　如果在一个包含着 Σ 的任意环中, 关系式 (13.36) 和 (13.37) 成立, 其中 $\delta_{S,T} \neq 0$, 则 u_S 或者全为零, 或者在 Σ 上线性无关.

证　假定某个 u_S 与另外某几个线性无关的 u_T 线性相关, 那么 (对这一个 S 来说) 有

$$u_S = \sum_{T \neq S} u_T \gamma_T. \tag{13.41}$$

将 (13.41) 式右乘 β^S 即有

$$u_S \beta^S = \sum_T u_T \gamma_T \beta^S, \tag{13.42}$$

将 (13.41) 左乘 β, 则由 (13.36) 有

$$u_S \beta^S = \sum_T u_T \beta^T \gamma_T. \tag{13.43}$$

由于 u_T 这些元素已经假定为线性无关的, 故比较 (13.42) 和 (13.43) 可得

$$\beta^T \gamma_T = \gamma_T \beta^S,$$

或

$$\gamma_T(\beta^T - \beta^S) = 0. \tag{13.44}$$

由于 $T \neq S$, 故可找到一个 β, 使 $\beta^T \neq \beta^S$. 这时 (13.44) 给出 $\gamma_T = 0$. 这一情况对出现于 (13.41) 中的一切 T 均成立, 因此应有 $u_S = 0$. 这时由 (13.37) 可以推出 $u_{ST} = 0$ 对一切 T 成立, 也就是说一切 u_S 都等于零.

从刚才所证定理可以推出:

$\mathfrak{A}$ 是单代数, 也就是说, 在 $\mathfrak{A}$ 中除了 $\{0\}$和 $\mathfrak{A}$ 自身之外没有其他双边理想.

事实上, 如果 $\mathfrak{m}$ 是一个双边理想, 则 $\mathfrak{A}/\mathfrak{m}$ 是一个环, 其中的同余类 $\bar{u}_S$ 满足方程 (13.36) 和 (13.37), 因此这些 $\bar{u}_S$ 或者全为零, 或者在 Σ 上线性无关. 在第一种情形下, 有 $\mathfrak{m} = \mathfrak{A}$, 而在第二种情形下 $\mathfrak{m}=\{0\}$.

总括起来, 有下面的结论: 叉积 $\mathfrak{A}$ 是 P 上的一个中心单代数.

循环代数

如果 Galois 群 $\mathfrak{G}$ 是一个循环群, 则叉积 $\mathfrak{A}$ 称为 P 上的一个循环代数. 在这一情形下, $\mathfrak{G}$ 中一切元素 T 都是同一生成元 S 的幂:

$$T_k = S^k \quad (k = 0, 1, \cdots, n-1).$$

我们可以取 u_S 的幂作为 u_T：

$$u_T = (u_S)^k \quad (k = 0, 1, \cdots, n-1). \tag{13.45}$$

u_T 的这种取法是和我们在前面所提出的那样一个要求相吻合的，即取 $\mathfrak{A}$ 中的单位元 e 作为 u_E：

$$u_E = (u_S)^0 = e.$$

u_S 的 n 次幂就是它的 $(n-1)$ 次幂和一次幂的乘积. 因此，由 (13.27) 可得

$$u_S^n = e\delta, \tag{13.46}$$

其中 δ 为 Σ 中的一个元素. 这样一个元素就决定了整个因子系，因为当 $i+k<n$ 时，有

$$u_S^i \cdot u_S^k = u_S^{i+k},$$

而当 $i+k \geqslant n$ 时有

$$u_S^i \cdot u_S^k = u_S^{i+k-n} \cdot u_S^n = u_S^{i+k-n}\delta,$$

这就是说，因子 $\delta_{T,R}$ 或者等于 1，或者等于 δ，视 $T = S^i$ 和 $R = S^k$ 中指数之和 $i+h<n$ 或 $\geqslant n$ 而定.

将 (13.46) 左乘或右乘 u_S 可得

$$u_S^{n+1} = u_S\delta = \delta u_S,$$

因此，由 (13.36) 有

$$\delta = \delta^S.$$

这就是说，δ 在 $\mathfrak{G}$ 下不变，亦即 δ 属于 P. 如果这一条件成立的话，整个结合性条件 (13.41) 都成立. 因此，除了 $\delta \neq 0$ 和 $\delta \in P$ 之外，δ 不必再满足其他条件.

如果将 u_S 换成 $v_S = u_S\gamma$，则

$$\begin{aligned} v_S^n &= (u_S\gamma)(u_S\gamma)\cdots(u_S\gamma) \\ &= u_S^n\gamma\gamma^S\gamma^{S^2}\cdots\gamma^{S^{n-1}}. \end{aligned}$$

γ 的一切共轭元的积等于 γ 在 P 上的范数. 因此有

$$v_S^n = e\varepsilon, \quad \varepsilon = \delta N(\gamma). \tag{13.47}$$

这样，我们就有下面的结论：

域 P 上的一个循环代数 $\mathfrak{A}$, 作为循环域 Σ 和它的 Galois 群 $\mathfrak{G}$ 的叉积来说, 只要在基域 P 中给定一个元素 $\delta \neq 0$ 即可完全确定. 元素 δ 可以乘上 Σ 中一个任意元素 $\gamma \neq 0$ 的范数, 而不致改变代数 $\mathfrak{A}$.

按照 Hasse 的创议, 循环代数 $\mathfrak{A}$ 用记号 (δ, Σ, S) 来表示.

如果取 P 为一个特征 $\neq 2$ 的域, Σ 为 P 的一个二次扩域 $P(\sqrt{-\alpha})$, 并命 $\delta = -\beta$, 则所得到的循环代数就是例 2 中的广义四元数代数.

循环代数的结构虽然是如此简单, 可是仍具有很大的普遍意义. 事实上, Brauer, Hasse 和 Noether(*J. f. reine u. angew. Math.*, 167: 399) 曾经证明过这样一个 “基本” 定理. 这个定理断定, 有限次代数数域上的每个中心可除代数都是循环代数.

习题 13.4　一个环的中心仍是环.

习题 13.5　全阵环 P_n 是 P 上的一个中心单代数.

习题 13.6　如果一切因子 $\delta_{S,T} = 1$, 则 Σ 和 $\mathfrak{G}$ 的叉积等于 Σ 和 $\mathfrak{G}$ 的群环的积.

13.4　作为带算子群的代数, 模与表示

当我们把一个代数 $\mathfrak{A}$ 看成对加法来说的交换群时, 它容许如下两个算子区:

第一个算子区是域 P. 这一算子区之下的可许子群即一切*线性子空间*.

第二个算子区就是代数 $\mathfrak{A}$ 本身, 它的元素既可看成左算子, 也可看成右算子. 这时可许子群就是*左理想*、*右理想*和*双边理想*.

现在让我们一劳永逸地作出如下的约定: 即当我们考虑一个代数中的 (左、右或双边) 理想时, 我们永远把域 P 作为算子区一道考虑在内. 这就是说, 只有那样的子群才能算是*可许左想理*, 它们在包含每个元素 a 的同时, 不仅包含着一切元素 ra(r 属于 $\mathfrak{A}$), 而且也包含着一切元素 $a\beta$(β 属于 P). 右理想的情况也是如此. 因此, 可许理想永远同时是线性子空间. 同样, 两个左理想*算子同构*, 当且仅当二者之间存在一个同构对应, 它在将元素 a 映成 $\bar{a}$ 的同时, 也将每个 ra 映成 $r\bar{a}$, 每个 $a\beta$ 映成 $\bar{a}\beta$. 一个左理想称为*单左理想*或*极小左理想*, 如果这个左理想除了它自身和零理想之外, 不包含其他可许左理想.

对理想概念加上这样一个限制之后, 一个代数中的理想满足*极大和极小条件*:

每个非空的 (左、右或双边) 理想集合 (至少) 包含一个极大理想, 即那样一个理想, 它不再包含在同一集合中的另一理想之内, 也 (至少) 包含一个极小理想, 它不再包含同一集合中的其他理想.

事实上, 根据我们的约定, 每个理想同时也是一个子空间, 而在秩 $\leqslant n$ 的子空间的每个非空集合中必有一个秩最大和秩最小的子空间.

为了在尽可能一般的假设之下得出代数理论中的许多基本定理, 在整个这一章的过程中我们不再局限于考虑某个域上的代数, 而是考虑任意的环 $\mathfrak{o}$. 对于这样的

环, 我们可以根据不同的需要加上左理想或右理想的极大或极小条件. 环 $\mathfrak{o}$ 还可以带上一个算子区 Ω(它取代早先的域 P 的作用), 其中的算子 $\beta, \gamma, \cdots$ 具有性质:

$$(a+b)\beta = a\beta + b\beta, \tag{13.48}$$

$$(ab)\beta = (a\beta)b = a(b\beta). \tag{13.49}$$

如果存在着这样一个算子区, 那么理想的概念必须和前面一样受到如下一个限制, 即每个理想在包含 a 的同时, 也包含着一切 $a\beta$(β 属于 Ω). 如果我们希望把这一点明确地强调出来, 我们就采用**可许**左或右理想等说法. 极大或极小条件只要对这种理想成立就行.

其次必须弄清楚理想理论中的哪一些概念, 如理想的和、积等等, 对带有或不带有算子区的非交换环仍不失去其意义. 首先容易看出, 两个可许右或左理想的交 $\mathfrak{a}\cap\mathfrak{b}$与和 $(\mathfrak{a},\mathfrak{b})$仍是可许右或左理想. 此外还可以立即看出, 积$\mathfrak{ab}$(即一切和 $\sum ab$ 的集合, $a \in \mathfrak{a}, b \in \mathfrak{b}$) 是一个可许右理想, 如果其中第二个因子为可许右理想; 是一个可许左理想, 如果其中第一个因子为可许左理想. 另一因子可以是 $\mathfrak{o}$ 中一个完全任意的集合或个别的元素. 举例来说, 只要 $\mathfrak{b}$ 是一个右理想, $p\mathfrak{b}$, 即一切乘积 $pa(a \in \mathfrak{b})$ 的集合, 便是一个右理想.

如果 $\mathfrak{a}$ 是 $\mathfrak{o}$ 中的一个左理想, 而 $\mathfrak{c}$ 为 $\mathfrak{o}$ 中任意集合, 那么我们可以定义**左商** $\mathfrak{a}:\mathfrak{c}$为 $\mathfrak{o}$ 中具有性质

$$x\mathfrak{c} \subseteq \mathfrak{a}$$

的元素 x 的集合.

左商仍然是一个左理想. 事实上, 由 $x\mathfrak{c} \subseteq \mathfrak{a}$ 和 $y\mathfrak{c} \subseteq \mathfrak{a}$ 可以推出 $(x-y)\mathfrak{c} \subseteq \mathfrak{a}$, 而由 $x\mathfrak{c} \subseteq \mathfrak{a}$ 可以推出 $rx\mathfrak{c} \subseteq r\mathfrak{a} \subseteq \mathfrak{a}$ 对 $\mathfrak{o}$ 中一切元素 r 成立. 如果 $\mathfrak{a}$ 和 $\mathfrak{c}$ 都是左理想, 那么 $\mathfrak{a}:\mathfrak{c}$ 甚至还是一个双边理想. 事实上, 由 $x\mathfrak{c} \subseteq \mathfrak{a}$ 可以推出 $xr\mathfrak{c} \subseteq x\mathfrak{c} \subseteq \mathfrak{a}$. 两个右理想的右商可以类似定义, 可是我们不会用到它.

为了说明极小条件有多大的限制性, 我们证明以下的定理:

定理 设 $\mathfrak{o}$ 是一个满足左理想极小条件的环, a 是 $\mathfrak{o}$ 中的一个元素, 并且不是 $\mathfrak{o}$ 中的一个右零因子, 那么在 $\mathfrak{o}$ 中方程 $xa = b$ 对任意 b 可解.

证 左理想 $\mathfrak{o}\mathfrak{a}^n (n = 1, 2, \cdots)$ 的集合中必有一个极小者. 设为 $\mathfrak{o}a^m$. 由于 $\mathfrak{o}a^{m+1} \subseteq \mathfrak{o}a^m$, 而 $\mathfrak{o}a^{m+1} \subset \mathfrak{o}a^m$ 的可能性已被排除, 故必有 $\mathfrak{o}a^{m+1} = \mathfrak{o}a^m$. 因此每个乘积 ba^m 都可以写成 ca^{m+1} 的形式:

$$ba^m = ca^{m+1}.$$

于是可以从等式左右两端消去 m 个因子 a, 故有

$$b = ca,$$

这就是说, 方程 $xa = b$ 有解.

定理 如果 $\mathfrak{o}$ 是一个满足右理想极小条件的环, 而 a 不是左零因子, 则方程 $ax = b$ 可解.

将这两个定理结合起来可以推出：

如果 $\mathfrak{o}$ 是一个满足左理想和右理想极小条件的无零因子环, 则 $\mathfrak{o}$ 必是一体.

特别, 任何一个无零因子的代数是一个体. 此种代数称为可除代数.

习题 13.7 对于一个具有单位元的环来说, 上面所提到的由于算子区 P 或 Ω 的存在而对理想概念所加上的限制是不起作用的：每个理想都能容许 P 或 Ω 的作用.

习题 13.8 环 $\mathfrak{o}$ 中左理想的极大和极小条件成立的充分必要条件是 $\mathfrak{o}$ 中存在左理想的合成列.

除了 $\mathfrak{o}$ 中的理想之外, 我们还要考虑 $\mathfrak{o}$ 模, 特别是 $\mathfrak{o}$ 的元素作为左算子的模 $\mathfrak{M}$. 我们称此种模为 $\mathfrak{o}$ 左模. 设 $\mathfrak{o}$ 的元素为 $a, b, \cdots$; $\mathfrak{M}$ 的元素为 $u, v, \cdots$. 这时应有

$$a(u+v) = au + av, \tag{13.50}$$

$$(a+b)u = au + bu, \tag{13.51}$$

$$(ab)u = a(bu). \tag{13.52}$$

如果环 $\mathfrak{o}$ 还带有一个算子区 Ω, 那么我们要求 $\mathfrak{M}$ 也能容许 Ω 中算子的作用(这些算子我们写在 $\mathfrak{M}$ 中的元素的右边), 并要求运算规则

$$(u+v)\beta = u\beta + v\beta, \tag{13.53}$$

$$(au)\beta = a(u\beta) = (a\beta)u \tag{13.54}$$

成立. 这样一来, 所考虑的模就是一个双模($\mathfrak{o}$ 左, Ω 右).

谈到模 $\mathfrak{M}$ 的子模时, 所指的永远是可许的子模, 即能够容许 $\mathfrak{o}$ 和 Ω 中的算子作用的子模. 如果一个模 $\mathfrak{M}$ 除了 $\{0\}$ 和 $\mathfrak{M}$ 之外不再有其他子模, 这个模就称为一个单模 或极小模. 环 $\mathfrak{o}$ 称为单环, 如果它作为一个以 $\mathfrak{o}$ 为右算子区和左算子区 (可能还要带上某个附加的算子区 Ω) 的双模来说是一个单模, 也就是说, 它除了 $\{0\}$ 和 $\mathfrak{o}$ 之外不再具有其他可许双边理想.

以 $\mathfrak{o}$ 中的一个元素 a 去乘 $\mathfrak{M}$ 中的元素, 就给出 Ω 模 $\mathfrak{M}$ 的一个自同态 A：

$$au = Au. \tag{13.55}$$

这样一来, $\mathfrak{o}$ 中的每个元素 a 都有一个自同态 A 与之相当. 与积 ab 相当的自同态是积 AB, 而与和 $a+b$ 相当的自同态是和 $A+B$. 后者由

$$(A+B)u = Au + Bu \tag{13.56}$$

定义. 因此, 对应 $a \to A$ 是一个环同态. 如果对任意 $\beta \in \Omega$, 我们用

$$(A\beta)u = (Au)\beta \tag{13.57}$$

来定义自同态 $A\beta$, 那么积 $A\beta$ 和积 $a\beta$ 相当. 因此环同态 $a \to A$ 同时还是一个相对于 Ω 来说的算子同态. 具有这一性质的一个环同态称为 $\mathfrak{o}$ *的一个表示* ($\mathfrak{o}$ 的元素表示成 Ω 模 $\mathfrak{M}$ 的自同态).

我们已经看到, 每一个 (以 $\mathfrak{o}$ 为左算子区, Ω 为右算子区的) 双模 $\mathfrak{M}$ 都给出 $\mathfrak{o}$ 的一个表示. 反之, 如果给定了 $\mathfrak{o}$ 的一个表示 $a \to A$, 它将 $\mathfrak{o}$ 的元素 a 表示成 Ω 模 $\mathfrak{M}$ 的自同态 A, 那么只要利用 (13.55) 来定义乘积 au, 就可以将 $\mathfrak{M}$ 转变成为一个以 $\mathfrak{o}$ 为左算子区, Ω 为右算子区的双模.

如果 $\mathfrak{o}$ 是基域 Ω 上的一个代数, 因而是 Ω 上的一个向量空间, 那么在大部分情况之下我们只考虑那样的模 $\mathfrak{M}$, 对它们来说, Ω 中的单位元同时也是单位算子. 换句话说, $\mathfrak{M}$ 也必须是 Ω 上的向量空间. 这时前面所讲到的自同态就是向量空间 $\mathfrak{M}$ 的线性变换, 而我们所讨论的也就是 $\mathfrak{o}$ *的线性变换表示*.

同态 $a \to A$ 的核由所有满足条件 $a\mathfrak{M} = \{0\}$ 的元素组成, 即核等于双边理想 $\{0\}$:$\mathfrak{M}$. 如果核等于零理想, 即所考虑的同态为一同构, 我们就说这样一个表示是*忠实的*.

表示 $a \to A$(像在 12.4 节中所定义的那样) 称为*可约的*, 如果表示模 $\mathfrak{M}$ 具有一个异于 $\{0\}$ 和 $\mathfrak{M}$ 的子模 $\mathfrak{N}$. 如果不存在这样的子模, 即 $\mathfrak{M}$ 为一单模, 那么表示 $a \to A$ 就称为*不可约的*.

如果模 $\mathfrak{M}$ 在 7.6 节的意义之下完全可约, 即可表成一些单模的直和, 我们就说表示 $a \to A$ 是*完全可约的*. 一个可约的或完全可约的方阵表示中方阵的具体形状如何, 这一点由公式 (12.14) 和 (12.17) 作了解答.

如果一个环 $\mathfrak{o}$ 的两个表示是由彼此同构的两个模给出的, 这两个表示就称为*等价的表示*. 在有限维向量空间的情形下, 这就是说, 只要在表示模中相应地选取基向量, 就可使两个表示具有相同的方阵.

这里所建立的各种关系虽然非常简单, 它们对代数的结构与表示理论有着非常重大的意义. 早在 13.2 节的例 2 中我们就得出了四元数的一个两行两列的方阵表示, 而所用的办法恰恰就是把四元数代数 $\mathfrak{A}$ 本身看成一个 ($\mathfrak{A}$ 左, Σ 右) 双模.

13.5 小根与大根

一个 (左或右) 理想 $\mathfrak{a}$ 称为*幂零的*, 如果它的某个幂 $\mathfrak{a}^m$ 是零理想 $\{0\}$. 我们有

引理 1 *两个幂零左理想的和* (a, b) *是幂零左理想.*

证　设 $\mathfrak{a}^m = \mathfrak{b}^n = \{0\}$. 将理想 $(\mathfrak{a}, \mathfrak{b})^{m+n-1}$ 具体展开出来可得到一个和, 其中每一项都是 $m+n-1$ 个 $\mathfrak{a}$ 或 $\mathfrak{b}$ 之积. 在这样一个乘积中或者因子 $\mathfrak{a}$ 出现至少 m 次, 或者因子 $\mathfrak{b}$ 出现至少 n 次. 比方说, 如果第一种情况出现, 那么这个乘积具有形式:

$$\cdots \mathfrak{a} \cdots \mathfrak{a} \cdots \mathfrak{a} \cdots ,$$

其中至少有 m 个因子 $\mathfrak{a}$. 可是 $\mathfrak{o}\mathfrak{a} \subseteq \mathfrak{a}$, 故有

$$\cdots \mathfrak{a} \cdots \mathfrak{a} \cdots \mathfrak{a} \cdots \subseteq \mathfrak{a}^m \cdots = \{0\}.$$

因此一切乘积均为 $\{0\}$, 故有

$$(\mathfrak{a}, \mathfrak{b})^{m+n-1} = \{0\}.$$

引理 2　*每个幂零左或右理想都包含在一个幂零双边理想之内.*

证　设 $\mathfrak{l}$ 是一个幂零左理想. $\mathfrak{l}^n=\{0\}$. 这时 $\mathfrak{l}$ 也是幂零的:

$$(\mathfrak{l}\mathfrak{o})^n = \mathfrak{l}(\mathfrak{o}\mathfrak{l})^{n-1}\mathfrak{o} \subseteq \mathfrak{l}\mathfrak{l}^{n-1}\mathfrak{o} = \mathfrak{l}^n\mathfrak{o} = \{0\}.$$

这样一来, 由 $\mathfrak{l}$ 所生成的右理想 $(\mathfrak{l}, \mathfrak{l}\mathfrak{o})$ 就是两个幂零左理想之和, 因而它本身也是一个幂零左理想, 即一个幂零双边理想.

环 $\mathfrak{o}$ 的小根 $\mathfrak{N}$ 指的就是 $\mathfrak{o}$ 中一切幂零双边理想之并. 根据引理 2, 一切幂零左理想和右理想都包含在这个并内, 因此我们也可以把 $\mathfrak{N}$ 定义为一切幂零左理想 (或右理想) 之并. 此外还有另一种说法: a 属于 $\mathfrak{N}$ 当且仅当 a 生成一个幂零左理想 (或右理想).

当 $\mathfrak{o}$ 为一代数, 或者更广一点, 为一满足左理想极小条件的环时, 小根 $\mathfrak{N}$ 和下面将要定义的大根 $\mathfrak{R}$ 相一致. 在这一情况下我们可去掉 “小” 字, 而将 $\mathfrak{R} = \mathfrak{N}$ 称为代数 $\mathfrak{o}$ 的根.

一个无根的代数, 即根等于零理想的代数, 称为半单代数. 半单代数的结构已由 MacLagan-Wedderburn 阐明. 他的主要定理是:

定理　*每个半单代数都是一些具有单位元的单代数的直和, 而每个这样的单代数都同构于一个体上的全阵环.*

Artin(*Abh. Math. Sem. Univ., Hamburg,* 5: 245) 将 Wedderburn 的定理推广到满足左理想极小条件的环. 如果不加上这样一个条件, 要想得出简单的结构定理是不可能的. 其原因就是根 $\mathfrak{N}$ 还太小了. 这一点早就有人指出过. 许多作者, 其中包括 Baer 和 Levitzki 等人, 曾经定义了环的大根. 可是一直到 Jacobson 才在大根 $\mathfrak{R}$ 的一个适当定义的基础之上, 成功地得出了无根环的结构定理. 关于整个这一理

论的一个全面的叙述, 可参看 Jacobson 的书 *Structure of Rings* (1956). 这里我们仅限于介绍几个主要定理.

Jacobson 在他的书中将一个环 $\mathfrak{o}$ 的大根 $\mathfrak{R}$ 定义为那样一些元素 a 的集合, 它们在 $\mathfrak{o}$ 的每个不可约表示之下都被映成零. 进一步, Jacobson 证明, 大根 $\mathfrak{R}$ 也可以作为某些被它称之为 "范式" 理想的极大右理想的交得出. 这里的右理想可以换成左理想. 此种更动对大根并无影响. 在本节中我们利用范式极大左理想来定义环的大根.

左理想 $\mathfrak{L}$ 称为一个范式 (modular) 理想, 如果在 $\mathfrak{o}$ 中可以找到一个元素 c, 使得

$$ac \equiv a(\mathfrak{L}) \tag{13.58}$$

对 $\mathfrak{o}$ 中一切元素 a 成立.

元素 c 在某种意义上起着 mod $\mathfrak{L}$ 的右单位元的作用, "modular" 这个字导源于 "module" 一词, 这就是单位元的较老的名称①.

现在我们定义环 $\mathfrak{o}$ 的大根, 或者简短一点, 环 $\mathfrak{o}$ 的根, $\mathfrak{R}$ 为 $\mathfrak{o}$ 中一切范式极大左理想 $\mathfrak{L}$ 之交. 如果在 $\mathfrak{o}$ 中除了 $\mathfrak{o}$ 本身之外没有范式极大左理想, 根 $\mathfrak{R}$ 就和整个环相重合. 这样的环称为根环.

现设 $\mathfrak{L}$ 为一个范式极大左理想. 同余类模 $\mathfrak{o}/\mathfrak{L}$ 是一个单模, 从而给出 $\mathfrak{o}$ 的一个不可约表示. 这一表示的核就是双边理想

$$\mathfrak{P} = \mathfrak{L} : \mathfrak{o}, \tag{13.59}$$

亦即一切具有性质

$$a\mathfrak{o} \subseteq \mathfrak{L} \tag{13.60}$$

的元素 a 的全体.

性质 (13.60) 等价于

$$ab \in \mathfrak{L}, \text{ 对一切 } b \in \mathfrak{o}. \tag{13.61}$$

特别, 由 (13.60) 可得出 $ac \in \mathfrak{L}$, 从而根据 (13.58) 有 $a \in \mathfrak{L}$. 这一事实对 $\mathfrak{P}$ 中一切元素 a 成立, 因此有

$$\mathfrak{P} \subseteqq \mathfrak{L}. \tag{13.62}$$

对每个 $\mathfrak{L}$ 有一个 $\mathfrak{P} = \mathfrak{L} : \mathfrak{o}$. 根据 (13.62) 一切 $\mathfrak{P}$ 的交包含在一切 $\mathfrak{L}$ 的交之内, 亦即包含在根 $\mathfrak{R}$ 之内. 现在我们反过来证明, $\mathfrak{R}$ 包含在每个理想 $\mathfrak{P}$ 之内, 因而也包含在它们的交之内.

① 本书中采用的译名没有照顾这一意义. —— 校者

设 a 为 $\mathfrak{R}$ 中的一个元素. 我们要证明条件 (13.61) 对任意 b 和 $\mathfrak{L}$ 成立, 也就是说, 要证明 a 包含在每个左理想

$$\mathfrak{L}' = \mathfrak{L} : b$$

之内. 可是 a 属于 $\mathfrak{o}$ 以及 $\mathfrak{o}$ 中的每个范式极大左理想, 因此要想证明这样一个事实, 只要证明 $\mathfrak{L}'$ 或者等于 $\mathfrak{o}$, 或者为 $\mathfrak{o}$ 中的范式极大左理想就行.

对于固定的 b 和 $\mathfrak{L}$ 来说, $\mathfrak{o}$ 中每个元素 x 都有一个乘积 xb 和一个 mod $\mathfrak{L}$ 的同余类 $xb+\mathfrak{L}$ 与之相应. 这样一个对应是一个模同态. 这个同态的核恰是 $\mathfrak{L}' = \mathfrak{L} : b$. 因此, $\mathfrak{o}/\mathfrak{L}'$ 被同构地映入 $\mathfrak{o}/\mathfrak{L}$. 另一方面, $\mathfrak{o}/\mathfrak{L}$ 是一个单模, 因此我们只有以上两种可能的情况：或者 $\mathfrak{o}/\mathfrak{L}'$ 被同构地映射成零, 从而它本身为一零模, 或者 $\mathfrak{o}/\mathfrak{L}'$ 被同构地映射成整个 $\mathfrak{o}/\mathfrak{L}$. 在第一种情况下有 $\mathfrak{L}' = \mathfrak{o}$, 在第二种情况下 $\mathfrak{L}'$ 和 $\mathfrak{L}$ 一样都是 $\mathfrak{o}$ 中的范式极大左理想.

总结起来我们有以下的定理.

定理 1　*根 $\mathfrak{R}$ 等于双边理想 $\mathfrak{P} = \mathfrak{L} : \mathfrak{o}$ 的交, 因而其自身为一双边理想.*

现在我们作同余类环 $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{R}$. $\mathfrak{o}$ 中的每个范式极大左理想 $\mathfrak{L}$ 都有 $\bar{\mathfrak{o}}$ 中一个范式极大左理想 $\bar{\mathfrak{L}} = \mathfrak{L}/\mathfrak{R}$ 与之相对应. 反之亦然. 因此我们有

定理 2　*同余类环 $\mathfrak{o}/\mathfrak{R}$ 是一个无根环, 也就是说, $\mathfrak{o}/\mathfrak{R}$ 的根是零理想.*

无根环称为半单的. 因此定理 2 可改述如下：

环 $\mathfrak{o}$ 对它的根 $\mathfrak{R}$ 的同余类环是一个半单环

习题 13.9　如果 $\mathfrak{o}/\mathfrak{L}'$ 与 $\mathfrak{o}/\mathfrak{L}$ 算子同构, 则

$$\mathfrak{L}' : \mathfrak{o} = \mathfrak{L} : \mathfrak{o} = \mathfrak{P}.$$

习题 13.10　如果 $\mathfrak{L}$ 为一个范式左理想, 则 $\mathfrak{J} = \mathfrak{L} : \mathfrak{o}$ 是一个包含在 $\mathfrak{L}'$ 之内的双边理想, 它包含着一切包含在 $\mathfrak{L}$ 之内的双边理想.

在下文中我们要用到下面这样一个定理：

定理 3　*每个范式左理想 $\mathfrak{l} \neq \mathfrak{o}$ 均可扩张为一极大左理想 $\mathfrak{L} \neq 0$(后者自然仍是范式理想).*

证　设 c 为环 $\mathfrak{o}$ 中具有性质

$$ac \equiv a(\mathfrak{l}), \quad 对一切\ a \in \mathfrak{o} \tag{13.63}$$

的元素. 左理想 $\mathfrak{l}$ 不包含 c. 考虑一切包含着 $\mathfrak{l}$ 而不包含元素 c 的左理想 $\mathfrak{l}'$ 的集合. 我们要在这些左理想 $\mathfrak{l}'$ 当中找出一个极大的 $\mathfrak{L}$ 来. 根据 Zorn 引理 (9.2 节), 这样的理想存在. 这个 $\mathfrak{L}$ 是范式理想, 因为它包含 $\mathfrak{l}$. 它又是极大的, 并且 $\neq \mathfrak{o}$. 事实上, 如果 $\mathfrak{L}$ 有一个真包理想 $\mathfrak{L}'$, 则 $\mathfrak{L}'$ 将包有元素 c, 从而根据 (13.63) 包有 $\mathfrak{o}$ 中的每个元素 a.

为了研究小根和大根之间的关系, 我们要引入一种新的乘法来作为辅助工具.

13.6 星　积

环 $\mathfrak{o}$ 中两个元素 a 和 b 的*星积* $a*b$ 由

$$a*b=a+b-ab$$

定义. Jacobson 把它写成 $a\circ b$, 并把这一运算称为 "圆合成".

星积满足结合律, 环中的零元是星乘法之下的单位元：

$$0*a=a*0=a.$$

如果 $\mathfrak{o}$ 有单位元 1, 那么 $a*b=c$ 也可以由

$$(1-a)(1-b)=1-c$$

来定义, 由此立即得出星乘法的结合性.

一个给定元素 z 的*左星逆元* z' 由

$$z'*z=0 \quad 或 \quad z'+z-z'z=0$$

定义, 而当 $\mathfrak{o}$ 中存在单位元 1 时, 可由

$$(1-z')(1-z)=1$$

定义. 具有左星逆元 z' 的元素 z 称为*左星正则元*(或左拟正则元). 同样, 由条件 $z*z'=0$ 可定义右星逆元和右星正则元的概念.

一个元素 z 称为*星正则*的, 如果可以找到一个元素 z', 它既是 z 的左星逆元, 也是它的右星逆元：

$$z'*z=0=z*z'.$$

定理 4　*每个幂零元是星正则的.*

证　设 $z^m=0$, 并命

$$z'=-z-z^2-\cdots-z^{m-1},$$

则有 $z'*z=0=z*z'$. 因此 z 为星正则元.

如果一个左理想 $\mathfrak{l}$ 中所有元素都是左星正则的, 那么它们一定都是星正则元素. 事实上, 设 z 为 $\mathfrak{l}$ 中一个元素, 并设 z' 为它的左星逆元, 则

$$z'=z'z-z.$$

因此, z' 包含在 $\mathfrak{l}$ 内, 从而根据我们的假设具有一左星逆元 z''. 这样一来, 就有

$$z = 0 * z = z'' * z' * z = z'' * 0 = z'',$$

即

$$z * z' = z'' * z' = 0,$$

这就是说, z' 不但是 z 的左星逆元, 而且也是它的右星逆元.

如果一个左或右理想中所有元素都是星正则的, 我们就说它是一个*星正则理想*. 根据以上所证, 对于一个左理想来说, 只要它的一切元素均为左星正则就够了. 同样, 对右理想来说只需要求它的一切元素均为右星正则元.

定理 5 *根 $\mathfrak{R}$ 是一个星正则左理想, $\mathfrak{o}$ 中一切星正则左理想都包含在 $\mathfrak{R}$ 之内.*

证 设 z 为 $\mathfrak{R}$ 中的一个元素. 我们要证明 z 具有一个左星逆元. 我们作一切形如

$$xz - x$$

的元素的集合, 其中 x 遍历整个环 $\mathfrak{o}$. 这个集合是一个范式左理想, 其中元素 z 起着早先的元素 c 的作用. 如果这个左理想包含元素 z, 那么这就意味着存在一个元素 x, 使得

$$z = xz - x,$$

由此即有 $x * z = 0$, 亦即 x 为 z 的左星逆元. 如果这个范式左理想不包含 z, 那么它就不可能等于 $\mathfrak{o}$, 因而根据定理 3, 可以把它扩张成为一个范式极大左理想 $\mathfrak{L} \neq \mathfrak{o}$. 可是 z 属于 $\mathfrak{R}$, 而 $\mathfrak{R}$ 为一切范式极大左理想之交, 因此 z 属于 $\mathfrak{L}$. 这样一来, 一切元素

$$x = xz - (xz - x)$$

均属于 $\mathfrak{L}$, 也就是说, $\mathfrak{L}$ 等于 $\mathfrak{o}$. 而据 $\mathfrak{L}$ 的定义它是不等于 $\mathfrak{o}$ 的.

由此可见, $\mathfrak{R}$ 中每个元素 z 都有一个左星逆元. 因此 $\mathfrak{R}$ 为一星正则左理想.

现在假设 $\mathfrak{l}$ 为一星正则左理想. 我们要证明 $\mathfrak{l}$ 包含在一切范式极大左理想 $\mathfrak{L}$ 之内, 从而包含在 $\mathfrak{R}$ 之内.

假设 $\mathfrak{l}$ 不包含在 $\mathfrak{L}$ 内. 这时 $(\mathfrak{L}, \mathfrak{l})$ 将等于整个环 $\mathfrak{o}$:

$$(\mathfrak{L}, \mathfrak{l}) = \mathfrak{o}. \tag{13.64}$$

由于 $\mathfrak{L}$ 是范式左理想, 故可找到一个元素 c, 使

$$ac \equiv a(\mathfrak{L}), \quad 对一切\ a \in \mathfrak{o}. \tag{13.65}$$

由条件 (13.64), 这个元素 c 一定能表成和 $y+z$ 的形式, 其中 y 属于 $\mathfrak{L}$ 而 z 属于 $\mathfrak{l}$. 由此即有

$$c \equiv z(\mathfrak{L}). \tag{13.66}$$

由于 z 属于 $\mathfrak{l}$, 它应有一个左星逆元 z':

$$z + z' - z'z = 0. \tag{13.67}$$

由 (13.66) 和 (13.67) 立得

$$c + z' - z'c \equiv 0(\mathfrak{L}),$$

从而由 (13.65) 有

$$c \equiv 0(\mathfrak{L}),$$

而这是不可能的.

由定理 5 很容易证明一个环中的左根和右根彼此相等. 事实上, 如果我们定义右根 $\mathfrak{R}'$ 为一切范式极大右理想之交, 则 $\mathfrak{R}'$ 将是一个星正则双边理想, 因而根据定理 5. 它应包含在 $\mathfrak{R}$ 之内. 同理可知, $\mathfrak{R}$ 包含在 $\mathfrak{R}'$ 之内, 从而有 $\mathfrak{R} = \mathfrak{R}'$. 这样一来, 我们就可以根据自己的意愿将根 $\mathfrak{R}$ 或者定义为一切范式极大左理想或右理想之交, 或者定义为一切星正则左理想或右理想之并.

一个左或右理想称为一个*幂零元理想*, 如果它的一切元素都是幂零元. 由定理 4 可知, 每个幂零元理想是星正则的, 从而由定理 5 可得

定理 6 *一切幂零元理想均包含在根 $\mathfrak{R}$ 之内.*

特别, 一切幂零理想包含在 $\mathfrak{R}$ 之内. 一切幂零理想的并集即环中的小根 $\mathfrak{N}$. 因此我们有

定理 7 *小根 $\mathfrak{N}$ 包含在大根 $\mathfrak{R}$ 之内.*

习题 13.11 环 $\mathfrak{o}$ 的一个左或右单位元不可能是星正则的, 因而不会包含在根 $\mathfrak{R}$ 之内.

13.7 满足极小条件的环

从现在起我们假定环 $\mathfrak{o}$ 满足左理想的极小条件. 在这一假设之下首先证明:

定理 8 *大根 $\mathfrak{R}$ 是幂零的.*

证 在由 $\mathfrak{R}$ 的各个幂 $\mathfrak{R}^m$ 所构成的序列中必有一个极小的理想 $\mathfrak{R}^n$. 由于 $\mathfrak{R}^{2n}$ 包含在 $\mathfrak{R}^n$ 之内, 故必有

$$\mathfrak{R}^{2n} = \mathfrak{R}^n.$$

如命 $\mathfrak{R}^n = \mathfrak{S}$, 则有 $\mathfrak{S}^2 = \mathfrak{S}$. 我们要证明 $\mathfrak{S} = \{0\}$.

假设 $\mathfrak{S} \neq \{0\}$. 我们考虑一切具有性质

$$\mathfrak{I} \subseteq \mathfrak{S}, \tag{13.68}$$

$$\mathfrak{S}\mathfrak{I} \neq \{0\} \tag{13.69}$$

的左理想 $\mathfrak{I}$ 的集合.

这一集合是非空的, 因为 $\mathfrak{S}$ 本身就是这样一个左理想. 因此, 具有性质 (13.68) 和 (13.69) 的左理想当中必有一极小者 $\mathfrak{I}_m$. 由于 (13.69), 在 $\mathfrak{I}_m$ 中可找到一个元素 b, 使 $\mathfrak{S}b \neq \{0\}$. 左理想 $\mathfrak{S}b$ 包含在 $\mathfrak{I}_m$ 之内, 并且具有性质 (13.68) 和 (13.69), 因此 $\mathfrak{S}b = \mathfrak{I}_m$. 由此可知, 在 $\mathfrak{S}$ 中可找到一个元素 z, 使 $zb = b$, 由于 z 属于 $\mathfrak{R}$, 故据定理 5, 元素 z 有一左星逆元 z':

$$z + z' - z'z = 0. \tag{13.70}$$

将这个方程右乘 b, 即得 $b = 0$. 而这是和我们的假设 $\mathfrak{S}b \neq \{0\}$ 相违背的. 这就证明了 $\mathfrak{S} = \{0\}$, 亦即 $\mathfrak{R}^n = \{0\}$.

小根 $\mathfrak{N}$ 包含一切幂零双边理想, 因此有 $\mathfrak{N} \supseteq \mathfrak{R}$. 另一方面, 由定理 7 有 $\mathfrak{N} \subseteq \mathfrak{R}$. 这样一来就得出了

定理 9 *小根 $\mathfrak{N}$ 等于大根 $\mathfrak{R}$.*

根据定理 6, 一切幂零元理想包含在 $\mathfrak{R}$ 之内, 因此有

定理 10 *一切幂零元理想是幂零理想.*

定理 2 告诉我们, 同余类环 $\mathfrak{o}/\mathfrak{R}$ 是半单的. 如果左理想的极小条件在 $\mathfrak{o}$ 中成立, 那么它在 $\mathfrak{o}/\mathfrak{R}$ 中也自然成立. 现在我们要一般地研究满足左或右理想极小条件的半单环.

定理 11 *每个满足左理想极小条件的半单环 $\mathfrak{o}$ 都是一些单 (极小) 左理想 $\mathfrak{l}_i$ 的直和.*

证 根据定义, $\mathfrak{o}$ 的根, 亦即 $\mathfrak{o}$ 中的零理想, 是一切范式极大左理想 $\mathfrak{L}$ 之交. 作为第一步, 我们首先证明, 只要从这些 $\mathfrak{L}$ 中取出有限多个出来作交, 就足以得出零理想来.

为此我们考虑一切能够表成有限多个范式极大左理想 $\mathfrak{L}$ 之交的左理想的集合. 这一集合中必有一个极小的左理想

$$\mathfrak{l} = \mathfrak{L}_1 \cap \cdots \cap \mathfrak{L}_m.$$

如果 $\mathfrak{l} \neq \{0\}$, 那么一定还可以找到一个 $\mathfrak{L}_{m+1}$, 它和 $\mathfrak{l}$ 的交是 $\mathfrak{l}$ 的一个真子集, 而这是和 $\mathfrak{l}$ 的极小性相违背的. 因此应有 $\mathfrak{l} = \{0\}$, 从而有

$$\{0\} = \mathfrak{L}_1 \cap \cdots \cap \mathfrak{L}_m. \tag{13.71}$$

如果在理想 $\{0\}$的这个交表示中出现一个 $\mathfrak{L}_i$, 它包含着其余各个理想之交, 那么在表示 (13.71) 中这样一个项 $\mathfrak{L}_i$ 就是多余的. 从 (13.71) 中去掉一切多余的 $\mathfrak{L}_i$, 最后便得出一个不可缩短的交表示:

$$(0) = \mathfrak{L}_1 \cap \cdots \cap \mathfrak{L}_n, \tag{13.72}$$

其中没有一个 $\mathfrak{L}_i$ 是包含其余各个理想之交 $\mathfrak{l}_i$ 的. 这样一来, 和 $(\mathfrak{L}_i, \mathfrak{l}_i)$ 就是 $\mathfrak{L}_i$ 的一个真包理想. 由于 $\mathfrak{L}_i$ 的极大性, 它应等于整个环 $\mathfrak{o}$:

$$(\mathfrak{L}_i, \mathfrak{l}_i) = \mathfrak{o}. \tag{13.73}$$

等式 (13.72) 和 (13.73) 说明, $\{0\}$是极大左理想 $\mathfrak{L}_i$ 的直交. 因此根据 13.1 节, $\mathfrak{o}$ 应是左理想 $\mathfrak{l}_i$ 的直和:

$$\mathfrak{o} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n. \tag{13.74}$$

其次, 根据 13.1 节, 我们有算子同构关系

$$\mathfrak{l}_i \cong \mathfrak{o}/\mathfrak{L}_i, \tag{13.75}$$

由于同余类模 $\mathfrak{o}/\mathfrak{L}_i$ 为单模, 故 $\mathfrak{l}_i$ 也是单的. 这就证明了我们的定理.

根据 (13.74), $\mathfrak{o}$ 中每个元素 a 可唯一地表成和:

$$a = a_1 + \cdots + a_n \quad (a_i \in \mathfrak{l}_i) \tag{13.76}$$

的形式.

我们可以在表示式 (13.76) 中突出一个项 a_i, 而把 (13.76) 写成

$$a = a_i + b_i \quad (a_i \in \mathfrak{l}_i, b_i \in \mathfrak{L}_i). \tag{13.77}$$

元素 a_i 称为 a 的 $\mathfrak{l}_i$ 分量. 对应 $a \to a_i$ 是一个算子同态, 其核恰为 $\mathfrak{L}_i$. 两个元素 a 和 a' 同余 $(\mathrm{mod}\ \mathfrak{L}_i)$, 当且仅当它们有相同的 $\mathfrak{l}_i$ 分量.

具有性质 $c^2 = c$ 的环元素 c 称为幂等元. 现在我们证明

定理 12 如果采用定理 11 中的假设和记号, 则

(1) 每个 $\mathfrak{l}_i$ 由一个幂等元 e_i 生成:

$$\mathfrak{l}_i = \mathfrak{o}e_i, \quad e_i^2 = e_i.$$

(2) 元素 e_i 相互零化:

$$e_i e_k = 0, \quad 对\ i \neq k. \tag{13.78}$$

(3) 任意元素 a 的 $\mathfrak{l}_i$ 分量 a_i 可以用 e_i 去右乘 a 得到

$$a_i = ae_i. \tag{13.79}$$

(4) 幂等元 e_i 之和

$$e = e_1 + \cdots + e_n \tag{13.80}$$

是 $\mathfrak{o}$ 中的单位元.

证 由于 $\mathfrak{L}_i$ 为范式理想, 故在 $\mathfrak{o}$ 中可找到一个元素 c_i, 使有性质

$$ac_i = a(\mathfrak{L}_i), \quad 对一切\ a \in \mathfrak{o}. \tag{13.81}$$

按公式 (13.77) 将 c_i 分解, 可得

$$c_i = e_i + f_i, \tag{13.82}$$

由此即得 ac_i 的分解式

$$ac_i = ae_i + af_i. \tag{13.83}$$

由同余式 (13.81) 可知, ac_i 和 a_i 有相同的 $\mathfrak{l}_i$ 分量. 因此, 由 (13.83) 式便有

$$a_i = ae_i. \tag{13.84}$$

这就证明了 (13.79). 如果令 a 遍及整个环 $\mathfrak{o}$, 则 a_i 遍历左理想 $\mathfrak{l}_i$, 因此有

$$\mathfrak{l}_i = \mathfrak{o}e_i. \tag{13.85}$$

在 (13.84) 中命 $a = e_i$, 立得

$$e_i = e_i^2. \tag{13.86}$$

在 (13.84) 中命 $a = e_k$, 则得

$$0 = e_k e_i \quad (k \neq i). \tag{13.87}$$

这就证明了断言 A, B 和 C.

命

$$e = e_1 + \cdots + e_n, \tag{13.88}$$

则由 (13.84) 可得

$$ae = ae_1 + \cdots + ae_n = a_1 + \cdots + a_n = a. \tag{13.89}$$

这就是说, e 是 $\mathfrak{o}$ 中的右单位元. 因此我们只要证明 e 同时也是左单位元就行了.

元素 $a-ea$ 组成一个右理想 $\mathfrak{r}$. 对任意元素 b, 我们有 $be=b$, 因此

$$b(a-ea)=ba-bea=ba-ba=0.$$

特别, 由此可得

$$(a-ea)^2=0.$$

因此 $\mathfrak{r}$ 为一幂零元理想. 根据定理 6, 它应包含在根之内, 也就是说, 应等于零. 因此对一切 a 有

$$a-ea=0,$$

亦即 e 为左单位元.

如果一个环作为左模来看是完全可约的, 即能表成一些单左理想的直和, 那么就称它为一个*左完全可约环*. 这样, 我们就可以把定理 11 和定理 12(4) 归并在一起, 而得到下面的结论:

每个满足左理想极小条件的半单环是左完全可约的, 并且具有单位元.

这个定理的逆也成立:

定理 13　*每个具有右单位元的左完全可约环是半单的, 并且满足左理想极小条件.*

证　设

$$\mathfrak{o}=\mathfrak{l}_1+\cdots+\mathfrak{l}_n \tag{13.90}$$

为将 $\mathfrak{o}$ 表成单左理想直和的分解. 如果命 $\mathfrak{L}_i$ 表除 $\mathfrak{l}_i$ 之外其余各个 $\mathfrak{l}_j$ 之和, 则有 $\mathfrak{o}/\mathfrak{L}_i\cong\mathfrak{l}_i$, 因而 $\mathfrak{L}_i$ 为一极大左理想. 设 e 为 $\mathfrak{o}$ 的右单位元, 则对一切 $a\in\mathfrak{o}$ 有 $ae=a$, 因此每个 $\mathfrak{L}_i$ 都是范式理想. 根据 13.1 节, 理想 $\mathfrak{L}_i$ 的交为 $\{0\}$, 因此 $\mathfrak{o}$ 为半单环.

由 7.6 节可知, $\mathfrak{o}$ 具有一个长度为 n 的合成列. 根据 7.4 节, 对每个左理想 $\mathfrak{l}$ 都可找到一个合成列, 使之以 $\mathfrak{l}$ 为一项. 合成列中由 $\mathfrak{l}$ 到 $\{0\}$的截段之长度为 $m\leqslant n$. 这个数 m 称为左理想 $\mathfrak{l}$ 的长度. $\mathfrak{l}$ 的一个真子理想 $\mathfrak{l}'$ 的长度必小于 $\mathfrak{l}$ 的长度, 因为我们可以作出 $\mathfrak{l}$ 的一个合成列, 使之以 $\mathfrak{l}'$ 为一项. 在任何一个左理想的非空集合中都有一个长度最小的左理想 $\mathfrak{l}''$. 这样一个左理想 $\mathfrak{l}''$ 就是该集合中的极小左理想, 因为 $\mathfrak{l}''$ 的真子理想 $\mathfrak{l}'''$ 的长度将会来得更小. 因此, 环 $\mathfrak{o}$ 中左理想的极小条件成立.

13.8　双边分解与中心分解

在 13.7 节中我们已经研究了在某些假设之下将环 $\mathfrak{o}$ 分解成左理想直和的问题. 现在让我们来看一看关于环 $\mathfrak{o}$ 分解成双边理想直和的问题.

定理 14 如果一个具有单位元的环 $\mathfrak{o}$ 能够表成一些不能再作双边直分解的非零双边理想的直和：

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n, \tag{13.91}$$

那么这些双边理想 $\mathfrak{a}_i$ 是唯一确定的.

证 如果我们有另一分解

$$\mathfrak{o} = \mathfrak{c}_1 + \cdots + \mathfrak{c}_m,$$

则

$$\mathfrak{c}_1 = \mathfrak{o}\mathfrak{c}_1 = (\mathfrak{a}_1\mathfrak{c}_1, \mathfrak{a}_2\mathfrak{c}_1, \cdots, \mathfrak{a}_n\mathfrak{c}_1).$$

由于

$$\mathfrak{a}_1\mathfrak{c}_1 \subseteq \mathfrak{a}_1, \cdots, \mathfrak{a}_n\mathfrak{c}_1 \subseteq \mathfrak{a}_n,$$

故上式右端的和是一个直和. 可是 $\mathfrak{c}_1$ 是不能再作双边直分解的, 故乘积 $\mathfrak{a}_i\mathfrak{c}_1$ 除去其中的一个 (譬如说 $\mathfrak{a}_1\mathfrak{c}_1$) 之外均应为零. 这样一来, 就有

$$\mathfrak{c}_1 = \mathfrak{a}_1\mathfrak{c}_1 \subseteq \mathfrak{a}_1.$$

由同样的推理可知, $\mathfrak{a}_1$ 反过来应包含在某个 $\mathfrak{c}_i$ 之内. 因此有

$$\mathfrak{c}_1 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{c}_i.$$

由此即得 $i = 1$ 和 $\mathfrak{c}_1 = \mathfrak{a}_1$. 因此每个 $\mathfrak{c}_i$ 都等于某个 $\mathfrak{a}_i$.

对单边直分解来说, 这样的唯一性定理不成立.

现在我们证明：

如果 $\mathfrak{o}$ 是双边理想 $\mathfrak{a}_i$ 的直和, 则 $\mathfrak{o}$ 的中心 $\mathfrak{z}$ 是环 $\mathfrak{a}_i$ 的中心 $\mathfrak{z}_i$ 的直和：

$$\mathfrak{z} = \mathfrak{z}_1 + \cdots + \mathfrak{z}_n.$$

证 设 $z = z_1 + \cdots + z_n$ 为 $\mathfrak{o}$ 的一个中心元素而 $x = x_1 + \cdots + x_n$ 为 $\mathfrak{o}$ 中任意元素, 则由 $zx = xz$ 可得

$$z_1x_1 + \cdots + z_nx_n = x_1z_1 + \cdots + x_nz_n. \tag{13.92}$$

由此即知 $z_ix_i = x_iz_i$ 对 $\mathfrak{a}_i$ 中一切 x_i 成立, 也就是说, z_i 属于 $\mathfrak{a}_i$ 的中心. 反之, 如果每个 z_i 都属于 $\mathfrak{a}_i$ 的中心, 则 (13.92) 对一切 x 成立, 因而有 $zx = xz$, 即 z 属于 $\mathfrak{o}$ 的中心.

上面这些论证对任意环 $\mathfrak{o}$ 成立. 现在我们假定 $\mathfrak{o}$ 是半单的, 并且满足左理想极小条件. 这时 $\mathfrak{o}$ 是左完全可约的：

$$\mathfrak{o} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n, \tag{13.93}$$

并有单位元

$$e = e_1 + \cdots + e_n \quad (e_i \in \mathfrak{l}_i). \tag{13.94}$$

设 $\mathfrak{a}$ 为 $\mathfrak{o}$ 中双边理想, 则每个 $\mathfrak{a}e_i$ 是包含在 $\mathfrak{l}_i$ 中的一个左理想. 因此 $\mathfrak{a}e_i$ 或者等于 $\mathfrak{l}_i$ 或者等于 $\{0\}$. 我们可以这样排列诸 $\mathfrak{l}_i$ 的顺序, 使得

$$\mathfrak{a}e_1 = \mathfrak{l}_1, \cdots, \mathfrak{a}e_m = \mathfrak{l}_m, \mathfrak{a}e_{m+1} = \{0\}, \cdots, \mathfrak{a}e_n = \{0\}.$$

这时 $\mathfrak{l}_1, \cdots, \mathfrak{l}_m$ 包含在 $\mathfrak{a}$ 内, 因而 $\mathfrak{l}_1 + \cdots + \mathfrak{l}_m$ 包含在 $\mathfrak{a}$ 内. $\mathfrak{a}$ 中的每个元素 a 等于

$$a = ae = ae_1 + \cdots + ae_n.$$

在这个和中 $ae_{m+1}, \cdots, ae_n$ 等于零, 因而整个和可缩成

$$a = ae_1 + \cdots + ae_m.$$

因此有 $\mathfrak{a} \subseteq \mathfrak{l}_1 + \cdots + \mathfrak{l}_m$, 即有

$$\mathfrak{a} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_m. \tag{13.95}$$

用文字表述出来, 这就是说:

每个双边理想 $\mathfrak{a}$ 都是某些个 $\mathfrak{l}_i$ 的和.

对于那些出现于 (13.95) 中的 $\mathfrak{l}_i$ 来说, 我们有

$$\mathfrak{a}\mathfrak{l}_i = \mathfrak{a}\mathfrak{o}e_i = \mathfrak{a}e_i = \mathfrak{l}_i;$$

与此相反, 对于那些不出现于 (13.95) 中的 $\mathfrak{l}_k$ 来说,

$$\mathfrak{a}\mathfrak{l}_k = \mathfrak{a}\mathfrak{o}e_k = \mathfrak{a}e_k = \{0\}.$$

由此可见, 出现于 (13.95) 中的那些 $\mathfrak{l}_i$ 可以由这样一个性质来刻画, 即它们不被 $\mathfrak{a}$ 所零化:

$$\mathfrak{a}\mathfrak{l}_i \neq \{0\}.$$

如果某一个 $\mathfrak{l}_i$ 有这种性质, 那么一切算子同构于 $\mathfrak{l}_i$ 的 $\mathfrak{l}_i$ 也有性质 $\mathfrak{a}\mathfrak{l}_j \neq \{0\}$. 因此, 与 $\mathfrak{l}_i$ 同时出现于 (13.95) 中的还有一切与它算子同构的 $\mathfrak{l}_j$.

现设 $\mathfrak{l}_1, \cdots, \mathfrak{l}_g$ 同构于 $\mathfrak{l}_1$, 而其余的 $\mathfrak{l}_j$ 不同构于 $\mathfrak{l}_1$. 那么我们可以断定:

$\mathfrak{a}_1 = \mathfrak{l}_1 + \cdots + \mathfrak{l}_g$是一个双边理想.

证 对任意 $b \in \mathfrak{o}$, 我们有

$$\mathfrak{a}_1 b = \mathfrak{a}_1 be = \mathfrak{a}_1(be_1 + \cdots + be_n)$$

$$\subseteq (\mathfrak{a}_1 be_1, \cdots, \mathfrak{a}_1 be_g, \cdots, \mathfrak{a}_1 be_n)$$
$$\subseteq (\mathfrak{l}_1, \cdots, \mathfrak{l}_g, 0, \cdots, 0) = \mathfrak{a}_1.$$

因此 $\mathfrak{a}_1$ 是一个右理想, 从而是一个双边理想.

按照这一方式, 由诸 $\mathfrak{l}_j$ 的每一个彼此同构的类可作出一个双边理想 $\mathfrak{a}_i$. 设所作出的双边理想为 $\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_r$.

注意每个双边理想 $\mathfrak{a}$ 都可表成一个形如 (13.95) 的直和. 并且如果这个和含有某一 $\mathfrak{l}_i$, 那么它也含有一切与它同构的 $\mathfrak{l}_j$. 因此我们有下面的结论:

每个双边理想 $\mathfrak{a}$ 都是双边理想 $\mathfrak{a}_1, \cdots, \mathfrak{a}_r$ 中某些个的直和. 后者为 $\mathfrak{o}$ 中的极小双边理想. 环 $\mathfrak{o}$ 可表成这些 $\mathfrak{a}_k$ 的直和:

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_r. \tag{13.96}$$

最后一项断言可由 (13.93) 直接得出.

根据 13.1 节, 诸 $\mathfrak{a}_i$ 是一些相互零化的环:

$$\mathfrak{a}_i \mathfrak{a}_k = \{0\}, \quad \text{对 } i \neq k. \tag{13.97}$$

由 (13.96) 和 (13.97) 可以看出, 环 $\mathfrak{a}_i$ 的每个左或右理想同时也是 $\mathfrak{o}$ 的左或右理想. 对于左理想 $\mathfrak{l}$ 来说, 这一点可以证明如下:

$$\mathfrak{o}\mathfrak{l} = (\mathfrak{a}_1 + \cdots + \mathfrak{a}_r)\mathfrak{l}$$
$$\subseteq (\mathfrak{a}_1\mathfrak{l}, \cdots, \mathfrak{a}_r\mathfrak{l})$$
$$\subseteq (0, \cdots, \mathfrak{a}_i\mathfrak{l}, 0, \cdots, 0) \subseteq \mathfrak{l}.$$

对右理想也可以同样地证明. 因此, $\mathfrak{a}_i$ 中的每个双边理想都是 $\mathfrak{o}$ 中的双边理想. 可是 $\mathfrak{a}_i$ 是 $\mathfrak{o}$ 中的极小双边理想, 从而 $\mathfrak{a}_i$ 中除了 $\mathfrak{a}_i$ 和 $\{0\}$之外不会再有其他双边理想. 因此 $\mathfrak{a}_i$ 是一个具有单位元 e_i 的单环. 这样, 我们就得到了

定理 15 *每个满足左理想极小条件的半单环都是一些具有单位元的单环的直和.*

对于代数 $\mathfrak{o}$ 来说, 这就是 13.5 节中所提出的 Wedderburn 定理的头一半.

现在我们研究具有单位元的单环.

13.9 单环与本原环

假设 $\mathfrak{o}$ 是一个具有右单位元 e 的单环:

$$ae = a, \quad \text{对一切 } a. \tag{13.98}$$

方程 (13.98) 表明, 零理想是一个范式左理想. 因此, 根据定理 3, 在 $\mathfrak{o}$ 中可找到一个范式极大左理想 $\mathfrak{L} \neq 0$. 同余类模 $\mathfrak{o}/\mathfrak{L}$ 是一个单模, 因而给出 $\mathfrak{o}$ 的一个不可约表示. 这个表示的核是一双边理想 $\mathfrak{P}$. 根据式 (13.62), $\mathfrak{P}$ 包含在 $\mathfrak{L}$ 之内, 因而有 $\mathfrak{P} \neq \mathfrak{o}$. 由于 $\mathfrak{o}$ 为单环, 故必有 $\mathfrak{P} = \{0\}$, 也就是说, 由 $\mathfrak{o}/\mathfrak{L}$ 所给出的表示是忠实的.

如果一个环具有一个忠实的不可约表示, 我们就说它是一个*本原环*. 这样, 我们就有

定理 16 *具有单位元的单环是本原环.*

现在让我们来看一看, 这个定理的逆命题是否成立.

设 $\mathfrak{o}$ 是一个本原环, 而 $\mathfrak{M}$ 是一个单 $\mathfrak{o}$ 模, 它给出 $\mathfrak{o}$ 的一个忠实表示. 设 u 是 $\mathfrak{M}$ 中一个不被 $\mathfrak{o}$ 所零化的元素, 则 $\mathfrak{o}u$ 将是 $\mathfrak{M}$ 的一个子模, 并且是不等于零的. 因此 $\mathfrak{o}u$ 应等于 $\mathfrak{M}$. 由 $x \to xu$ 可定义 $\mathfrak{o}$ 到 $\mathfrak{M}$ 之上的一个同态, 它的核是 $\mathfrak{o}$ 中的一个左理想 $\mathfrak{L}$. 同余类模 $\mathfrak{o}/\mathfrak{L}$ 同构于 $\mathfrak{M}$, 因而是一个单模. 由此可知 $\mathfrak{L}$ 为一极大左理想. 由于 $\mathfrak{o}u = \mathfrak{M}$, 故 u 本身可表成 cu 的形式：

$$u = cu.$$

由此可得 $au = acu$ 对 $\mathfrak{o}$ 中一切 a 成立. 因此, 元素 a 和 ac 在对应 $x \to xu$ 之下被映成 $\mathfrak{M}$ 中同一元素. 由此即得

$$a \equiv ac(\mathfrak{L}),$$

这就是说, $\mathfrak{L}$ 是一个范式左理想.

因为同构 $\mathfrak{M} \cong \mathfrak{o}/\mathfrak{L}$ 成立, 由 $\mathfrak{M}$ 所给出的表示与由 $\mathfrak{o}/\mathfrak{L}$ 所给出的表示等价. 这一表示的核是双边理想

$$\mathfrak{P} = \mathfrak{L} : \mathfrak{o}.$$

可是我们所考虑的表示是忠实的, 所以应有 $\mathfrak{P} = \{0\}$. 根据定理 1, 环 $\mathfrak{o}$ 的根 $\mathfrak{R}$ 包含在 $\mathfrak{P}$ 之内, 因此有 $\mathfrak{R} = \{0\}$. 这就是说, 环 $\mathfrak{o}$ 是半单的. 这样一来, 我们就有

定理 17 *本原环 $\mathfrak{o}$ 是半单的.*

在这个证明的第一部分中, 表示的忠实性尚未充分利用. 所用到的只有模 $\mathfrak{M}$ 的单性以及并非 $\mathfrak{M}$ 中一切元素均被 $\mathfrak{o}$ 所零化这一事实. 因此, 对任意环 $\mathfrak{o}$ 下面的定理成立.

定理 18 *每个不被 $\mathfrak{o}$ 所零化的单 $\mathfrak{o}$ 模 $\mathfrak{M}$ 同构于 $\mathfrak{o}$ 对某个范式极大左理想 $\mathfrak{L}$ 的同余类模 $\mathfrak{o}/\mathfrak{L}$. 如果由 $\mathfrak{M}$ 所给出的表示的核为 $\mathfrak{P}$, 则根 $\mathfrak{R}$ 包含在 $\mathfrak{P}$ 内, 也就是说, $\mathfrak{R}$ 中每个元素在这个表示下被映成零.*

现在让我们仍旧回到本原环上来. 如果假定环 $\mathfrak{o}$ 满足左理想极小条件, 那么由 $\mathfrak{o}$ 的半单性可知, $\mathfrak{o}$ 可表成一些极小左理想的直和：

$$\mathfrak{o} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n.$$

至少应有一个 $\mathfrak{l}_i$ 不包含在 $\mathfrak{L}$ 之内, 因为不然的话, 和 $\mathfrak{o}=\mathfrak{l}_1+\cdots+\mathfrak{l}_n$ 将会包含在 $\mathfrak{L}$ 内, 而这是不可能的. 对这样一个 $\mathfrak{l}_i$ 来说, 和 $(\mathfrak{l}_i,\mathfrak{L})$ 应等于 $\mathfrak{o}$, 因为 $\mathfrak{L}$ 是极大理想, 而交 $\mathfrak{l}_i\cap\mathfrak{L}$ 应为零, 因为 $\mathfrak{l}_i$ 是极小理想. 因此我们有同构关系：

$$\mathfrak{o}/\mathfrak{L}\cong\mathfrak{l}_i.$$

这就是说, 模 $\mathfrak{M}$ 同构于一个极小左理想 $\mathfrak{l}_i$, 而由 $\mathfrak{M}$ 所给出的表示同构于由 $\mathfrak{l}_i$ 所给出的表示.

根据 13.8 节, $\mathfrak{o}$ 是一些双边理想 $\mathfrak{a}_v$ 的直和, 这些双边理想, 除了其中的一个之外, 在由 $\mathfrak{l}_i$ 所给出的表示下都应被映成零. 由表示的忠实性可知, 只可能有一个 $\mathfrak{a}_v$, 也就是说, $\mathfrak{o}$ 本身是一个具有单位元的单环. 这样我们就有

定理 19　*每个满足左理想极小条件的本原环是单环, 并且具有单位元.*

定理 16 和定理 19 结合在一起表明, 对于满足左理想极小条件的环, 特别对于代数来说, “本原” 和 “单且具有单位元” 这两个性质是彼此等价的.

Jacobson 深入地阐明了一般本原环 (即不附加极小条件) 的结构. 每个本原环 $\mathfrak{o}$ 可以如此地嵌入一个向量空的线性变换环 $\mathfrak{D}$ 中去, 使得 $\mathfrak{o}$ 在 $\mathfrak{D}$ 中一种完全确定的拓扑结构之下以 $\mathfrak{D}$ 为闭包[①]. 这里我们只构造出这样一个向量空间, 并证明 $\mathfrak{o}$ 可以嵌进 $\mathfrak{D}$ 中去.

在这一构造中, $\mathfrak{o}$ 模的自同态环起着非常重要的作用. $\mathfrak{o}$ 模 $\mathfrak{M}$ 的自同态 L 就是 $\mathfrak{M}$ 到它自身之内的一个映射, 它具有性质：

$$L(u+v)=Lu+Lv, \tag{13.99}$$

$$L(au)=a(Lu). \tag{13.100}$$

性质 (13.100) 说明, 映射 L 和由 $\mathfrak{M}$ 所给出的表示 $a\to A$ 中的变换 A 可交换：

$$LA=AL,\quad 对一切\ A.$$

如果 $\mathfrak{M}$ 还带有另外一个算子区 Ω, 那么除了 (13.99) 和 (13.100) 之外, 我们还要求

$$L(u\beta)=(Lu)\beta \tag{13.101}$$

对 Ω 中一切 β 成立. 举例来说, 如果 Ω 为一域, 而 $\mathfrak{M}$ 是这个域上的同量空间, 则性质 (13.99),(13.100) 和 (13.101) 说明, 自同态 L 是 $\mathfrak{M}$ 的线性变换, 并且这个线性变换和表示 $a\to A$ 中的一切线性变换可交换.

如果像 6.9 节中所作的那样定义自同态的和与积：

$$(L+M)u=Lu+Mu,$$

① Jacobson N. *Structure of Rings*, 1956, 第 II 章.

$$(LM)u = L(Mu),$$

则自同态的全体形成一环, 即模 $\mathfrak{M}$ 的*自同态环*.

在下文中将会看到, 将自内态写成右算子 $\lambda, \mu, \cdots$, 并由

$$u(\lambda\mu) = (u\lambda)\mu$$

来定义它们的乘积, 经常是比较方便的. 采用这种写法时, 代替 (13.99)~(13.101) 我们有

$$(u+v)\lambda = u\lambda + v\lambda, \tag{13.102}$$

$$(au)\lambda = a(u\lambda), \tag{13.103}$$

$$(u\beta)\lambda = (u\lambda)\beta, \quad 对\ \beta \in \Omega. \tag{13.104}$$

右自同态也组成一个环, 即 $\mathfrak{o}$ 模 $\mathfrak{M}$ 的*右自同态环*. 在本节以及下一节中讲到一个模的自同态环时, 指的都是右自同态环. 右自同态环和左自同态环*反同构*. 这就是说, 每个左自同态 L 有一个唯一的右自同态 λ 与之相对应, 与和 $L+M$ 相对应的是和 $\lambda+\mu$, 而与积 LM 相对应的则是相反的积 $\mu\lambda$.

单 $\mathfrak{o}$ 模的自同态环是一体 K.

自同态环自然具有单位元, 这就是模的恒等自同构 ι. 因此, 只要证明, 每个自同态 $\lambda \neq 0$ 有一逆 λ^{-1} 即可. 自同态 λ 将 $\mathfrak{M}$ 映成一个子模 $\mathfrak{M}\lambda$. 如果 $\lambda \neq 0$, 那么这个子模不会是零子模, 因而必须等于 $\mathfrak{M}$. 被 λ 映成 0 的元素的集合也是 $\mathfrak{M}$ 的一个子模. 如果 $\lambda \neq 0$, 那么这一子模不会等于 $\mathfrak{M}$, 因而必须等于零模. 这样, 自同态 λ 就把 $\mathfrak{M}$ 同构地映成其自身, 因而它有一个逆自同构 λ^{-1}. 这就证明了上述断言.

体 K 称为单 $\mathfrak{o}$ 模 $\mathfrak{M}$ 的*自同态体*. 由于 K 的单位元 ι 是单位算子, 所以 $\mathfrak{M}$ 是 K 上的向量空间. 设 a 为 $\mathfrak{o}$ 中的元素, 则因为

$$a(u+v) = au + av,$$

$$a(u\lambda) = (au)\lambda,$$

所以 a 诱导出向量空间 $\mathfrak{M}$ 的一个线性变换 A. 对应 $a \to A$ 是一个环同态. 如果这一表示是忠实的, 则对应 $a \to A$ 为一同构, 这时环 $\mathfrak{o}$ 就被嵌进向量空间 $\mathfrak{M}$ 的线性变换环 $\mathfrak{D}$ 中去了.

习题 13.12 在环 $\mathfrak{o}$ 的一个完全可约表示之下, 大根 $\mathfrak{R}$ 永远被映成零.

习题 13.13 如果一个单环不是本原环, 那么它只能是那样的一个加法单群, 其中所有乘积 ab 均为零.

习题 13.14 不具有单位元的单代数必定是一个一维向量空间 a_1P, 其中 $a_1^2 = 0$.

13.10 直和的自同态环

设 $\mathfrak{M} = \mathfrak{M}_1 + \cdots + \mathfrak{M}_n$ 是 n 个单模的直和. 我们要对模 $\mathfrak{M}$ 的自同态环加以研究.

如果把 $\mathfrak{M}$ 中的一个元素 u 分解成它的 $\mathfrak{M}_i$ 分量：

$$u = u_1 + \cdots + u_n, \tag{13.105}$$

那么每个对应 $u \to u_i$ 都是 $\mathfrak{M}$ 的一个自同态 κ_i. 这些自同态的和就是 $\mathfrak{M}$ 的单位自同态 ι：

$$\iota = \kappa_1 + \cdots + \kappa_n. \tag{13.106}$$

这样一来, 每个自同态 μ 都可作如下的分解：

$$\begin{aligned}\mu = \iota\mu\iota &= \left(\sum \kappa_h\right)\mu\left(\sum \kappa_h\right)\\ &= \sum_{h,i} \kappa_h\mu\kappa_i.\end{aligned}$$

如果命

$$\kappa_h\mu\kappa_i = \mu_{hi}, \tag{13.107}$$

则有

$$\mu = \sum_{h,i} \mu_{hi}. \tag{13.108}$$

每个自同态 μ_{hi} 将 $\mathfrak{M}_h$ 映成 $\mathfrak{M}_i$, 而将所有其余的 $\mathfrak{M}_k (k \neq h)$ 映成零. 因此我们可以说, μ_{hi} 是从 $\mathfrak{M}_h$ 到 $\mathfrak{M}_i$ 的一个同态. (13.108) 中 n^2 个同态 μ_{hi} 是可以任意选取的, 它们的和给出 $\mathfrak{M}$ 的一个自同态 μ, 并且每个 μ 都可以用这种方式得出. 将 μ 表成从 $\mathfrak{M}_h$ 到 $\mathfrak{M}_i$ 的同态 μ_{hi} 之和的分解是唯一的, 因为将 (13.108) 式左乘 κ_h, 右乘 κ_i 就可立即得出 (13.107).

如果 $\mu = \sum \mu_{hi}$ 和 $\nu = \sum \nu_{hi}$ 是 $\mathfrak{M}$ 的两个自同态, 那么很容易作出它们的和与积. 这里只需注意, 当 $i \neq j$ 时 $\mu_{hi}\nu_{jk}$ 等于零. 这样便有

$$\mu + \nu = \sum_{h,i} (\mu_{hi} + \nu_{hi}), \tag{13.109}$$

$$\mu\nu = \sum_{h,k} \left(\sum_i \mu_{hi}\nu_{ik}\right). \tag{13.110}$$

同态 μ_{hi} 可以排成一个方阵 (μ_{hi}) 的形式. 这样一来, 每个自同态 μ 都有一个由同态 μ_{hi} 构成的方阵与之相当, 而后者是可以任意选择的. 根据 (13.109), 与和 $\mu + \nu$ 相当的是两个方阵之和, 而据 (13.110), 与积 $\mu\nu$ 相当的是两个方阵的积.

一般说来, 同态 μ_{hi} 中有许多是等于零的. 事实上, 我们有下面的定理:

如果 $\mathfrak{M}_h$ 被同态地映入 $\mathfrak{M}_i$, 而这个同态映射不是零映射, 那么它必是 $\mathfrak{M}_h$ 到 $\mathfrak{M}_i$ 之上的一个同构.

证 同态映射的核是 $\mathfrak{M}_h$ 的一个子模. 因此, 如果 $\mathfrak{M}_h$ 不全映成零的话, 这个核应等于 $\{0\}$. $\mathfrak{M}_h$ 的像是 $\mathfrak{M}_i$ 中的一个子模. 因此, 如果这个像不为 $\{0\}$的话, 它应等于整个 $\mathfrak{M}_i$.

由这个定理推出, $\mu_{hi}=0$, 除非 $\mathfrak{M}_h\cong\mathfrak{M}_i$. 现在我们把各个模 $\mathfrak{M}_i$ 分成一些彼此同构的类, 并且给它们作如此的编号, 使得 $\mathfrak{M}_1,\cdots,\mathfrak{M}_q$ 彼此同构, $\mathfrak{M}_{q+1},\cdots,\mathfrak{M}_{q+r}$ 彼此同构, 余类推. 这样一来, 方阵 (μ_{hi}) 就显然分裂成一些 $q,r,\cdots$ 阶方块, 而这些方块之外的系数全为零:

$$\begin{pmatrix} \boxed{\begin{matrix}\mu_{11} & \cdots & \mu_{1q}\\ \vdots & & \vdots \\ \mu_{q1} & \cdots & \mu_{qq}\end{matrix}} & & \\ & \boxed{\begin{matrix}\mu_{q+1,q+1} & \cdots & \mu_{q+1,q+r}\\ \vdots & & \vdots \\ \mu_{q+r,q+1} & \cdots & \mu_{q+r,q+r}\end{matrix}} & \\ & & \ddots \end{pmatrix}.$$

如果在第一个方块中写上任意的元素，而在所有其余的方块中写上零，那么我们就得出一个方阵环 E_1, 它是原有方阵环 E 的子环. 同样, 如果除第二个方块之外, 在所有其余位置都写上零, 那么便可得到一个环 E_2. 余此类推. 显然, E 中的每个元素可唯一地表成 $E_1,E_2,\cdots$ 中的元素之和, 并且 $E_1,E_2,\cdots$ 中的元素相互零化. 这就是说, *环 E 是一些彼此相互零化的环 $E_1,E_2,\cdots$ 的直和.*

这样一来, 为了弄清楚 E 的结构, 只要研究每个单个的 E_i 就行了. E_1 中的每个元素有第一个方块中的 q 阶方阵

$$\begin{pmatrix} \mu_{11}\cdots\mu_{1q}\\ \vdots \qquad \vdots \\ \mu_{q1}\cdots\mu_{qq}\end{pmatrix} \tag{13.111}$$

与之相对应.

μ_{11} 是 $\mathfrak{M}_1$ 的自同态体 K_1 中的一个元素. 其余的 μ_{hi} 不属于这一体, 而是 $\mathfrak{M}_h$ 到 $\mathfrak{M}_i$ 的同态. 可是我们可以把这些同态一对一地映射到 K_1 的元素上去. 其办法如下：取 q 个固定的同构

$$\mu_1,\cdots,\mu_q,$$

它们分别把 $\mathfrak{M}_1, \cdots, \mathfrak{M}_q$ 映成 $\mathfrak{M}_1$, 其中我们取 μ_1 为 $\mathfrak{M}_1$ 的恒等自同构. 对每个 μ_{hi}, 命元素

$$\lambda_{hi} = \mu_h^{-1}\mu_{hi}\mu_i \tag{13.112}$$

与之相对应. 这样一个元素是属于 K_1 的, 因为 μ_h^{-1} 将 $\mathfrak{M}_1$ 映成 $\mathfrak{M}_h$, μ_{hi} 将 $\mathfrak{M}_h$ 映成 $\mathfrak{M}_i$, 而 μ_i 将 $\mathfrak{M}_i$ 映成 $\mathfrak{M}_1$. 显然, 与和 $\mu_{hi}+\nu_{hi}$ 相对应的将是两个元素之和, 而与 (13.110) 中出现的那样乘积 $\mu_{hi}\nu_{ik}$ 相对应的将是两个元素之积. 这样一来, 每个方阵 (13.111) 都有一个系数属于 K_1 的方阵与之相对应, 和对应于和, 积对应于积. 这就是说, 环 E_1 同构于系数属于体 K_1(单模 $\mathfrak{M}_1$ 的自同构体) 的 q 阶全阵环.

总结以上所述, 我们得到

自同态环的结构定理　一个完全可约模 $\mathfrak{M}$ 的自同态环是体 K_i 上的全阵环 E_i 的直和.

13.11　半单环与单环的结构定理

我们从一个具有右单位元 e：

$$ae = a, \quad 对一切\ a$$

的环 $\mathfrak{o}$ 出发. 将 $\mathfrak{o}$ 看成一个以 $\mathfrak{o}$ 本身为左算子区的模, 并设法决定这个模的自同态 μ. 这样一个 μ 是环 $\mathfrak{o}$ 到它自身之内的一个映射, 它具有性质：

$$(a+b)\mu = a\mu + b\mu,$$

$$(ab)\mu = a(b\mu).$$

当 $b=e$ 时, 后一性质给出

$$a\mu = a(e\mu).$$

因此, 自同态 μ 可以用环 $\mathfrak{o}$ 中的一个元素 $d = e\mu$ 去作右乘而得出. 反之, 每个这样的右乘都是一个自同态：

$$(a+b)d = ad + bd,$$

$$(ab)d = a(bd).$$

因此, 自同态 μ 与环元素 d 一一对应, 并且和对应于和, 积对应于积. 这样就得出了下面的结论：

如果把一个具有右单位元 e 的环 $\mathfrak{o}$ 看成以 $\mathfrak{o}$ 为左算子区的模, 那么这个模的右自同态环同构于环 $\mathfrak{o}$ 本身.

作为这一定理的应用, 让我们决定一个满足左理想极小条件的半单环的结构. 根据定理 11, 这样一个环是一些单左理想的直和:

$$\mathfrak{o} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n. \tag{13.113}$$

根据 13.10 节, 这样一个直和的自同态环乃是某些体上的全阵环的直和. 另一方面, 根据 13.7 节, 环 $\mathfrak{o}$ 具有单位元. 因此我们有

半单环的结构定理 *每个满足左理想极小条件的半单环同构于某些体上的全阵环的直和.*

如果环 $\mathfrak{o}$ 是单环, 那么在这样一个直和表示中只能有一个全阵环出现. 因此有单环的结构定理如下:

每个具有单位元且满足左理想极小条件的单环同构于一个体 K 上的全阵环 K_n.

这里方阵的阶数 n 等于分解式 (13.113) 中左理想的个数. 由于 $\mathfrak{o}$ 是单环, 所有 $\mathfrak{l}_i$ 彼此同构. 体 K 就是其中一个 $\mathfrak{l}_i$ 的自同态体.

特别, 如果 $\mathfrak{o}$ 是某一域 P 上的单代数, 那么 P 中的元素 β 诱导出左理想 $\mathfrak{l}_i$ 的自同态 $x \to x\beta$, 因此我们可以把 P 嵌进自同态体 K 中去. 其次, 对于 K 中每个自同态 λ, 有

$$(x\beta)\lambda = (x\lambda)\beta,$$

因此 β 和 K 中每个 λ 可交换, 亦即 P 包含在 K 的中心之内. 由于全阵环 K_n 在 P 上的秩是有限的, 故 K 在 P 上有有限秩, 也就是说, K 是 P 上的一个可除代数. 这样我们就得出了

Wedderburn 定理 *每个具有单位元的单代数都同构于一个可除代数上的全阵环.*

下面每当我们谈到单代数的时候, 指的都是具有单位元的单代数, 因而可以看作一个可除代数上的全阵环. 单位元 e 的倍元 $e\beta$ 永远和 P 中的元素 β 相等同.

习题 13.15 体上全阵环的直和是半单环.

习题 13.16 体上的全阵环是单环和本原环.

习题 13.17 具有极小条件的交换半单环是域的直和.

13.12 代数在基域扩张下的动态

设 $\mathfrak{A}$ 是基域 P 上的一个半单代数. 我们要研究的是, 当基域 P 扩张成一个扩域 Λ 时, 代数 $\mathfrak{A}$ 将受到怎样的影响: $\mathfrak{A}$ 的哪些性质仍旧保持不变, 哪些性质将会消失? 我们的研究是按如下的程序来进行的: 先设 $\mathfrak{A}$ 为一域, 再设它为一可除代数,

其次再设它为一单代数, 最后才设它为一般的半单代数. 每次都是把下一个较为复杂的情况归结为前面较为简单的情况. 所考虑的环都假定具有单位元.

(1) 如果 $\mathfrak{A}$ 是 P 的一个有限可分扩域, 那么不论扩域 $\varLambda$ 怎样选择, $\mathfrak{A}_\varLambda$ 总是无根的. 反之, 如果 $\mathfrak{A}$ 是不可分的, 那么可以适当地选择 $\varLambda$, 使得 $\mathfrak{A}_\varLambda$ 有根.

证　设 $\mathfrak{A}$ 是可分的, θ 为 $\mathfrak{A}$ 的一个本原元 (6.10 节), $\varphi(z)$ 为以 θ 为零点的不可约多项式. 如果 $\varphi(z)$ 的次数为 n, 那么根据 6.3 节, 有

$$\mathfrak{A} = P + \theta P + \cdots + \theta^{n-1}P \cong P[z]/(\varphi(z)),$$

因而, 当基域扩张成 $\varLambda$ 时, 有

$$\mathfrak{A}_\varLambda = \varLambda + \theta\varLambda + \cdots + \theta^{n-1}\varLambda \cong \varLambda[z]/(\varphi(z)),$$

由于 $\varphi(z)$ 在 $\varLambda[z]$ 中也不会有重因子, 故在 $\varLambda[z]$ 中不可能找出这样一个多项式 $f(z)$ 来, 使得 $f(z)$ 的一个幂 $\equiv 0(\varphi(z))$, 而 $f(z)$ 本身 $\not\equiv 0(\varphi(z))$. 这就是说, 在 $\varLambda[z]/(\varphi(z))$ 中, 除了零元素之外, 没有幂零元. 根据定理 8, $\mathfrak{A}_\varLambda$ 的根全由幂零元组成. 由于在这个环中除零元之外没有幂零元素, 所以根应为零. 也就是说, $\mathfrak{A}_\varLambda$ 是一半单代数.

反过来, 如果 $\mathfrak{A}$ 是不可分的, 而 θ 是 $\mathfrak{A}$ 的一个不可分元素, 则 $\mathfrak{A}$ 有子域 $P(\theta)$, 而 $\mathfrak{A}_\varLambda$ 有子代数 $\varLambda(\theta)$. 和前面一样, 后者是同构于 $\varLambda[z]/(\varphi(z))$ 的. 适当地选择 $\varLambda$, 可使 $\varphi(z)$ 在 $\varLambda$ 中有重根, 因而在 $\varLambda[z]$ 中可找出一个多项式 $f(z)$ 来, 它本身不能被 $\varphi(z)$ 整除, 而它的一个幂能被 $\varphi(z)$ 整除. 因此在 $\varLambda(z)/(\varphi(z))$, 从而在与之同构的 $\varLambda(\theta)$ 中可以找出一个不等于零的幂零元来. 这个幂零元生成 $\mathfrak{A}_\varLambda$ 中的一个幂零元理想, 因为在一个交换环中每个幂零元都能生成一个幂零元理想. 这就证明了我们的定理.

由于 $\mathfrak{A}$ 和 $\varLambda$ 的地位是相互可易的, 故本定理的第一部分可以改述如下：如果域 $\mathfrak{A}$ 和 $\varLambda$ 中至少有一个是 P 的有限可分扩张, 则 $\mathfrak{A}\times\varLambda$ 是半单的. 由于 $\mathfrak{A}\times\varLambda$ 除了是半单代数之外还是可交换的, 故据习题 13.17, $\mathfrak{A}\times\varLambda$是域的直和.

(2) 现在让我们开始考虑 $\mathfrak{A}$ 为一体 K 的情形. 在下面的过渡定理的基础之上, 可以把这一情形归结为可交换的情形：

过渡定理　设 K 是 P 上的一个体, 其中心 $Z \supseteqq P$, 其次设 $\varLambda$ 为 P 上的一个代数, 并命 $\mathfrak{K} = K\times\varLambda, \mathfrak{Z} = Z\times\varLambda$, 则 $\mathfrak{K}$ 中每个双边理想 $\mathfrak{a}$ 都由 $\mathfrak{Z}$ 的一个双边理想生成.

如果把过渡定理稍加推广, 以一个模定理的形式把它表述出来, 它的意义就更容易看清楚.

设 K 为一体, 它具有某些个自同构 σ; 设 $\mathfrak{M}$ 为一有限秩 K 模：

$$\mathfrak{M} = z_1 K + \cdots + z_q K.$$

通过下面的定义

$$\sigma(z_1\kappa_1 + \cdots + z_q\kappa_q) = z_1(\sigma\kappa_1) + \cdots + z_q(\sigma\kappa_q),$$

K 的自同构 σ 也诱导出 $\mathfrak{M}$ 的自同构. 现在我们断言: *$\mathfrak{M}$ 的每个在诸自同构 σ 作用之下不变的子模 $\mathfrak{a}$ 必定有这样一个 K 基, 其中每个基元素在诸自同构 σ 的作用之下不变.*

证　设 $(z_1, \cdots, z_r)$ 为 $\mathfrak{a}$ 的一个 K 基. 根据 4.2 节, 我们可以添加若干个 z_i, 譬如说 $z_{r+1}, \cdots, z_q$, 把这个基补充成为 $\mathfrak{M}$ 的一个基. 这样一来, $\mathfrak{M}$ 中的每个元素 mod $\mathfrak{a}$ 同余于 $z_{r+1} \cdots z_q$ 的一个线性组合, 其系数属于 K. 特别对 $i = 1, 2, \cdots, r$ 有

$$z_i = \sum_{k=r+1}^{q} z_k \gamma_{ki} \pmod{\mathfrak{a}}.$$

如命

$$l_i = z_i - \sum_{k=r+1}^{q} z_k \gamma_{ki},$$

则 l_i 为 $\mathfrak{a}$ 中的线性无关元素. 事实上, 如果 l_i 之间存在某种线性关系, 则 $z_1 \cdots z_r$ 之间也将存在同样的线性关系, 而后者是线性无关的. 因此, $l_1, \cdots, l_r$ 构成 $\mathfrak{a}$ 的一个 K 基. 现在如果我们将自同构 σ 之一作用于 l_i, 那么就有

$$\sigma l_i = z_i - \sum_{r+1}^{q} z_k(\sigma\gamma_{ki}). \tag{13.114}$$

这个 σl_i 仍应属于 $\mathfrak{a}$, 因而必等于原有诸 l_i 的一个线性组合:

$$\sigma l_i = \sum l_j \alpha_j = \sum_{1}^{r} z_j \alpha_j - \sum_{r+1}^{q} z_k \sum_j \gamma_{kj} \alpha_j. \tag{13.115}$$

比较 (13.114) 和 (13.115) 可知, 除 $\alpha_i = 1$ 之外, 所有其余 $\alpha_j = 0$. 因此, $\sigma l_i = l_i$. 证毕.

为了从这个模定理得出我们所需要的过渡定理, 只要令模定理中所提到的自同构为 K 的全部内自同构 $\kappa \to \beta\kappa\beta^{-1}$ 即可. 事实上, 如果我们以 β 去作 $K \times \Lambda$ 中的元素的变换, 那么对 $z_1\kappa_1 + \cdots + z_q\kappa_q$ 这样的和来说, 这一变换的确是照以上所述方式起作用的: 它使得每个 z_i 不变而将 κ_i 变成 $\beta\kappa_i\beta^{-1}$. $K \times \Lambda$ 中的一个双边理想 $\mathfrak{a}$ 也是 K 模中的双边子模, 因而在自同构 $a \to \beta\mathfrak{a}\beta^{-1}$ 之下不变. 由此可知, $\mathfrak{a}$ 有一个这样的基, 它的每个基元素 $\sum z_i\kappa_i$ 在 β 的作用下不变, 亦即系数 κ_i 属于 K 的中心 Z. 因此, 这些基元素属于 $\mathfrak{Z} = Z \times \Lambda$. 过渡定理获证.

注 如果假定 K 在 P 上有有限秩, 那么将 Λ 换成任意体 Ω 时, 上述过渡定理仍然成立. 事实上, 设 $\mathfrak{a}$ 是 $\mathfrak{K} = K \times \Omega$ 中的一个双边理想, 则 $\mathfrak{a}$ 在 Ω 上和 $\mathfrak{K}$ 一样只可能有有限秩, 因而具有一个 Ω 基 $(a_1 \cdots, a_s)$. 如果把这些基元素都表成 $\sum \omega_i \kappa_i$ 这种形式, 那么总共只能出现有限多个 ω_i. 这些 ω_i 张成 Ω 的一个有限子模 Λ. 我们可以把模定理应用于积 $\mathfrak{M} = K \times \Lambda$ 及其子模 $\mathfrak{a} \cap \mathfrak{M}$, 从而得出子模 $\mathfrak{a} \cap \mathfrak{M}$ 的一个基, 其中每个基元素在 K 的一切内自同构之下不变, 亦即属于 $Z \times \Omega$. 这样一个基也就是 $\mathfrak{a}$ 的一个理想基.

从现在起, 我们假定 K 和 Λ 为 P 上的可除代数, 或 P 的有限扩域. 从过渡定理立即推出：

如果 $Z \times \Lambda$ 是单代数, 那么 $K \times \Lambda$ 也是单代数. 如果 $Z \times \Lambda$ 是半单的, 因而可以表成若干个单代数的直和, 那么 $K \times \Lambda$ 也是同样多个单代数的直和, 因而也是半单的.

正如 K 可以用它的中心来代替一样, Λ 自然也可以用它的中心来代替. 因此

如果 K 和 Λ 的中心之积是单代数或半单代数, 则 $K \times \Lambda$ 也同样是单代数或半单代数. 特别, 如果这两个中心之中有一个在 P 上是可分的, 则 $K \times \Lambda$ 是半单代数.

如果 K 是 P 上的中心代数, 即 $Z = P$, 则 $Z \times \Lambda = \Lambda$ 是一可除代数, 因而是单的. 因此

如果两个可除代数 K 和 Λ 中有一个是 P 上的中心代数, 则 $K \times \Lambda$ 是单代数.

(3) 由可除代数过渡到单代数, 即过渡到全阵环 $\mathfrak{A} = K_r$ 是很容易的. 设 Λ 是 P 上的一个任意的体, 我们有

$$\mathfrak{A} \times \Lambda = K_r \times \Lambda = K \times P_r \times \Lambda \cong (K \times \Lambda) \times P_r.$$

因此, 如果 $K \times \Lambda$ 是半单的, 因而是一些全阵环的直和, 那么为了得出 $\mathfrak{A} \times \Lambda$, 只要用 P_r 去和这些全阵环去作积, 也就是说, 只要将原有各个全阵环的阶数都乘上 r 就行了. 这一操作并不影响 $K \times \Lambda$ 的单性或半单性.

$\mathfrak{A} = K_r$ 的中心等于 K 的中心 Z. 因此我们有以下的定理：

如果 $\mathfrak{A} = K_r$ 的中心在 P 上是可分的, 则 $\mathfrak{A} \times \Lambda$ 是半单的. 如果 $\mathfrak{A}$ 是 P 上的中心单代数, 即 $Z = P$, 那么不论可除代数 Λ 为何, $\mathfrak{A} \times \Lambda$ 是单代数.

由过渡定理的注可知, 后一结果当 Λ 为 P 上的无限秩体时也成立.

(4) 每个半单代数 $\mathfrak{A}$ 是若干个单代数 $\mathfrak{A}', \mathfrak{A}'', \cdots$ 的直和. 用 Λ 去和每个被加的单代数作积, 就可得出积 $\mathfrak{A} \times \Lambda$. 特别, 如果我们取 Λ 为一域, 那么就有下面的结论：

半单代数在基域的每个可分扩张之下仍是半单的. 如果代数 $\mathfrak{A}', \mathfrak{A}'', \cdots$ 的中心都在 P 上可分, 那么这个代数的半单性在基域的任意扩张下不变.

(5) 我们看到, 一个单代数在基域扩张下的动态, 完全取决于作为该单代数的基础的可除代数的动态. 现在我们要对中心可除代数的动态作进一步的研究.

根据 (3) 中所证, 一个中心可除代数经过基域的扩张之后仍为中心单代数. 它不一定再是一个可除代数, 而可能变成某一体上的全阵环. 在这样的情况下, 我们说基域的扩张引起了可除代数的分裂(即分裂成单左理想).

我们证明: *如果 $K \neq P$ 是一个中心可除代数, 那么一定可以找到 P 的一个扩张, 使之造成 K 的分裂.*

事实上, β 为 K 中一个不属域 P 的元素. β 必是 $P[x]$ 中某个不可约多项式 $\varphi(x)$ 的零点. 在一个适当选择的域 Λ 中 $\varphi(x)$ 将成为可分解的. 例如, 我们可取 $\Lambda \cong P(\beta)$, 在这样的 Λ 中就可以分解出 $\varphi(x)$ 的一个一次因子. 根据前面所证, $\Lambda \times P(\beta) \cong \Lambda[x]/(\varphi(x))$, 因此 $\Lambda \times P(\beta)$ 中有零因子, 从而可以断定 $\Lambda \times K$ 中有零因子. 这样一来, 环 $\Lambda \times K$ 就不可能再是一个体, 它只可能是一个全阵环 $K'_{r'}(r' > 1)$.

比较等式 $K \times \Lambda = K'_{r'}$ 两边在 Λ 上的秩可得

$$(K : P) = {r'}^2 (K' : \Lambda),$$

其中记号 $(K : P)$ 表示 K 在 P 上的秩.

因此 K 在 Λ 上的秩一定比 K 在 P 上的秩来得小. 如果 $K' \neq \Lambda$, 那么我们又可以进一步作 Λ 的扩张, 使得 K' 再分裂. 这时 $K'_{r'}$ 将变成一个 $r'r''$ 阶全阵环. 一直这样进行下去, 由于体的次数越来越小, 最后必有一个终了的地步. 这样我们就得出一个完全分裂, 可除代数 K 变成了 Λ 上的一个全阵环:

$$K \times \Lambda \cong \Lambda_m.$$

具有这种性质的域 Λ 称为可除代数 Λ 的**分裂域**. 以上所证说明, 永远可以找到在 P 上的次数为有限的分裂域. 上面提到的关系式现在变成

$$(K : P) = m^2.$$

因此, 可除代数 K 在它的中心 P 上的秩永远是一个*完全平方数* m^2. 整数 m 即 K 作完全分裂时方阵的阶数, 这个数称为 K 的**指数**.

K 的分裂域也是 K_r 的分裂域, 反之亦然. 事实上, $K \times \Lambda$ 和 $K_r \times \Lambda$ 是同一体上的全阵环.

习题 13.18 如果 P 上两个单代数当中有一个是 P 上的中心单代数, 那么它们的积是单代数.

习题 13.19 P 的一个代数封闭扩域 Ω 是 P 上一切中心单代数的分裂域.

第 14 章　群与代数的表示论

14.1　问题的提出

设 $\mathfrak{G}$ 是一个群. 所谓群 $\mathfrak{G}$ 在域 K 中的一个表示, 指的就是一个群同态, 它把每个群元素 a 映射成 K 上一个 n 维向量空间中的线性变换 A (或者, 换一个说法, 映射成一个 n 阶方阵 A). 维数 n 称为表示的级数. 如果这个表示是一个同构, 它就称为一个忠实表示.

同样, 所谓环 $\mathfrak{o}$ 在 K 中的一个表示, 指的就是一个环同态 $a \to A$, 其中 A 仍是一个 n 维向量空间中的线性变换. 这个定义是和 12.4 节中所给的定义相一致的. 在 12.4 节中已经证明, $\mathfrak{o}$ 在 K 中的每个表示都有一个 ($\mathfrak{o}$ 左、K 右) 双模 $\mathfrak{M}$ 与之相当, $\mathfrak{M}$ 称为表示模. 反之, 每一个这样的双模都给出一个表示. 彼此同构的表示模给出相互等价的表示, 反之亦然. 一个表示称为可约的, 如果表示模中有一个不等于 $\{0\}$ 的真子模; 称为不可约的, 如果表示模是单模.

如果 $\mathfrak{o}$ 是 P 上的一个代数, 那么讲到 $\mathfrak{o}$ 的表示的时候我们还要求 P 包含在域 K 内, 并且, 由 $a \to A$ 即有 $a\beta \to A\beta$(对一切 $\beta \in P$). 对表示模 $\mathfrak{M}$ 来说, 这就意味着

$$(a\beta)u = (au)\beta, \quad 对一切 a \in \mathfrak{o}, \beta \in P, u \in \mathfrak{M}.$$

我们的主要问题是要找出一个已给群或代数的全部表示. 有限群的表示问题可以很容易地归结为代数的表示问题. 其办法就是以群 $\mathfrak{G}$ 中的元素 $a_1, \cdots, a_h$ 作为基元素, 按 13.2 节中所述方法作出这个群的群环

$$\mathfrak{o} = a_1 K + \cdots + a_h K.$$

如果 $a_i \to A_i$ 是群 $\mathfrak{G}$ 的一个表示, 那么很容易看出

$$\sum a_i \beta_i \to \sum A_i \beta_i$$

就是群环 $\mathfrak{o}$ 的一个表示. 反之, 群环 $\mathfrak{o}$ 的每个表示特别必将基元素 $a_1, \cdots, a_h$ 映射成某些线变换, 而这一映射就是群 $\mathfrak{G}$ 的一个表示. 因此

一个有限群在域 K 中的每个表示都可由群环的表示给出.

在代数的表示理论中, 我们通常假定表示域 K 和基域 P 相重合. 只要将 $\mathfrak{o}$ 扩张成 $\mathfrak{o}_K$, 就可以把一般的情形归结为这一特殊情形. 如果在原有的表示中 $\mathfrak{o}$ 的基元素

$a_1, \cdots, a_h$ 映成方阵 $A_1, \cdots, A_h$, 那么我们可以把 $\mathfrak{o}_K$ 中的一个元素 $\sum a_i\beta_i(\beta_i \in K)$ 映成方阵 $\sum A_i\beta_i$, 从而将 $\mathfrak{o}$ 的表示扩张成为 $\mathfrak{o}_K$ 的一个表示. 因此, $\mathfrak{o}$在域 K 中的每个表示可由 $\mathfrak{o}_K$ 的一个表示给出.

当环 $\mathfrak{o}$ 具有单位元时, 还要对问题的提法作进一步的限制. 在这样的情况下我们总是假定, 环中的单位元 1 同时也是表示模的单位算子, 也就是说, 这个元素在我们的表示下被映成单位方阵. 如其不然, 那么由 12.1 节可知, 表示模 $\mathfrak{M}$ 将分解成直和 $\mathfrak{M}_0 + \mathfrak{M}_1$, 其中 $\mathfrak{M}_0$ 被 $\mathfrak{o}$ 所零化, 而 $\mathfrak{M}_1$ 以 1 为单位算子. 这样一来, 整个表示就分裂成两个部分, 其中一个部分完全由零方阵组成, 因而是没有什么意义的; 另一部分给出一个表示, 它把单位元映成单位方阵.

代数的一个特别重要的表示, 就是所谓的*正则表示*. 这就是把 $\mathfrak{o}$ 本身看成表示模 ($\mathfrak{o}$ 左、P 右模) 所得到的表示. 如果所考虑的环左完全可约, 则正则表示完全可约.

14.2　代数的表示

在 13.9 节 (定理 18) 中我们已经看到, 代数 $\mathfrak{o}$ 的根 $\mathfrak{R}$ 在每个不可约表示之下被映成零. 这一事实对每个完全可约表示也成立, 因为每个完全可约表示都是把一些不可约表示并列起来得到的. 由于这个原因, 我们可以把 $\mathfrak{o}$ 的每个完全可约表示看作半单代数 $\mathfrak{o}/\mathfrak{R}$ 的表示.

下面的定理告诉我们, 怎样把一个半单代数的一切表示, 或者更一般一点, 把一个满足左理想极小条件的半单环的一切表示得出来. 根据 13.7 节, 每个这样的环 $\mathfrak{o}$ 都具有单位元, 并且是左完全可约的, 即可表成一些单左理想的直和. $\mathfrak{o}$ 的每个表示都由一个 $\mathfrak{o}$ 模给出. 有

主要定理　*设 $\mathfrak{o}$ 是一个具有单位元的左完全可约环, $\mathfrak{M}$ 是一个具有有限基的 $\mathfrak{o}$ 模. 其次假设 $\mathfrak{o}$ 的单位元是 $\mathfrak{M}$ 的单位算子. 这时 $\mathfrak{M}$ 必是一些单 $\mathfrak{o}$ 模的直和, 其中每个单模都同构于 $\mathfrak{o}$ 的一个单左理想.*

证　根据假设, 环 $\mathfrak{o}$ 是单左理想的直和:

$$\mathfrak{o} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_r. \tag{14.1}$$

又据假设, 模 $\mathfrak{M}$ 具有一个有限 $\mathfrak{o}$ 基 $(u_1, \cdots, u_s)$. 由此即得

$$\mathfrak{M} = (\mathfrak{o}u_1, \cdots, \mathfrak{o}u_s). \tag{14.2}$$

将 (14.1) 代入 (14.2) 得

$$\mathfrak{M} = (\cdots, \mathfrak{l}_i u_k, \cdots) \tag{14.3}$$

从 (14.3) 式右端的和中首先可以去掉那些等于零的模 $\mathfrak{l}_i u_k$. 另一方面, 如果 $\mathfrak{l}_i u_k \neq \{0\}$, 那么 $x \to xu_k$ 定义出 $\mathfrak{l}_i$ 到 $\mathfrak{l}_i u$ 上的一个算子同构. 因此不为零的模 $\mathfrak{l}_i u_k$ 同构于 $\mathfrak{l}_i$, 因而是单的. 如果某个 $\mathfrak{l}_i u_k$ 包含在其余各项的和之内, 那么我们可以从整个和中去掉这一项. 这一过程可以一直进行下去, 直到每个剩下来的项与其余各项的和只有零元素公共时为止. 这时所得和就是一个直和.

上述主要定理当 $\mathfrak{o}$ 和 $\mathfrak{M}$ 还带有一个满足附加条件

$$(au)\beta = a(u\beta) = (a\beta)u \quad (\beta \in \Omega)$$

的算子区 Ω 时自然也能成立. 应用于代数的表示理论时, Ω 是代数 $\mathfrak{o}$ 的基域 P, 这个域同时也是表示域. 如果 $\mathfrak{M}$ 是 P 上的有限维向量空间, 那么它自然具有一个有限 $\mathfrak{o}$ 基, 而这正是主要定理所要求的.

就半单代数来说, 这个定理表明, 这种代数的每个表示都是完全可约的, 并且它的每个不可约组成部分都已作为组成部分出现在正则表示之内. 事实上, 由 (14.1) 可以看出, 正则表示的不可约组成部分由单左理想 $\mathfrak{l}_i$ 给出.

根据 13.8 节, 每个半单代数 $\mathfrak{o}$ 可表成一些单代数 $\mathfrak{a}_\nu$ 的直和：

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s. \tag{14.4}$$

单代数 $\mathfrak{a}_\nu$ 又可以进一步分解成极小左理想 $\mathfrak{l}_i$ 的直和. 出现于同一 $\mathfrak{a}_\nu$ 中的 $\mathfrak{l}_i$ 彼此算子同构, 因而给出同一表示. 包含在 $\mathfrak{a}_\nu$ 之内的 $\mathfrak{l}_i$ 被每个 $\mathfrak{a}_\mu (\mu \neq \nu)$ 所零化：

$$\mathfrak{a}_\mu \mathfrak{l}_i \subseteq \mathfrak{a}_\mu \mathfrak{a}_\nu = \{0\}.$$

因此, 在由 $\mathfrak{l}_i$ 所给出的表示之下, 所有这些 $\mathfrak{a}_\mu$ 都被映成零, 只有 $\mathfrak{a}_\nu$ 得到一个忠实的表示. 事实上, $\mathfrak{a}_\nu$ 的表示的核是 $\mathfrak{a}_\nu$ 中的一个双边理想, 由于 $\mathfrak{a}_\nu$ 为单代数并且不全映成零, 所以核只可能是零理想.

现在我们研究一个单代数由它的一个任意的极小左理想所给出的表示.

根据 13.11 节, 具有单位元的单代数 $\mathfrak{o}$ 同构于一可除代数 Δ 上的全阵环. 设 c_{ik} 为 13.2 节中所引入的基本方阵 C_{ik}, 则

$$\mathfrak{o} = c_{11}\Delta + c_{12}\Delta + \cdots + c_{nn}\Delta.$$

通过

$$\mathfrak{l} = c_{11}\Delta + c_{21}\Delta + \cdots + c_{n1}\Delta$$

可给出 $\mathfrak{o}$ 中一个极小左理想 $\mathfrak{l}$. 基域 P 包含在 Δ 之内, 并且 Δ 在 P 上有有限秩. 所要考虑的表示将在 P 内给出.

先考虑 $\Delta = P$ 的情形. 这时我们可以利用 $\mathfrak{l}$ 的基 $(c_{11}, c_{21}, \cdots, c_{n1})$ 来明显地给出表示的方阵. 设 $a = \sum_{i,k=1}^{n} c_{ik}\alpha_{ik}$ 是 $\mathfrak{o}$ 中的一个元素, 则

$$ac_{k1} = \sum_{i=1}^{n} c_{ik}c_{k1}\alpha_{ik} = \sum_{i=1}^{n} c_{i1}\alpha_{ik}.$$

因此, 在由 $\mathfrak{l}$ 所给出的表示之下, 元素 a 被映成方阵 (α_{ik}). 由此可见, 代数 $\mathfrak{o}$ 与由方阵 (α_{ik}) 所组成的全阵环之间的同构, 恰恰就是由 $\mathfrak{o}$ 中一个极小左理想 $\mathfrak{l}$ 所给出的不可约表示.

值得注意的是, 在上面所讨论过的 $\Delta = P$ 的情形下, 表示方阵永远组成 n 阶全阵环. 这一事实也可以用另一方式来表述, 即表示方阵之中恰有 n^2 个线性无关的方阵.

现在假设 Δ 是 P 的一个真扩体.

$$\Delta = \lambda_1 P + \cdots + \lambda_r P.$$

在这一情况下我们首先作出 Δ 在 P 中的正则表示. 在这个正则表示下, Δ 中的元素 β 被映成由

$$\beta\lambda_j = \sum \lambda_i\beta_{ij}, \quad B = (\beta_{ij})$$

所定义的方阵 B. 其次作

$$\begin{aligned}\mathfrak{l} &= c_{11}\Delta + \cdots + c_{n1}\Delta \\ &= (c_{11}\lambda_1 P + \cdots + c_{11}\lambda_r P) \\ &\quad + \cdots + (c_{n1}\lambda_1 P + \cdots + c_{n1}\lambda_r P).\end{aligned}$$

利用这个基来作 $\mathfrak{o}$ 中元素 $c_{ik}\beta$ 的表示方阵, 就得到

$$c_{ik}\beta \to \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & B & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix},$$

其中, 零号代表 r 阶零方阵, 而 B 出现在第 i 行中的第 k 个位置上. 由此作和, 即得

$$\sum_{i,k}^{n} c_{ik}\alpha_{ik} \to \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix}, \tag{14.5}$$

其中, A_{ik} 仍是在 Δ 的正则表示之下与 α_{ik} 相当的方阵.

根据由 $\mathfrak{l}$ 所给出的不可约表示的具体形状还可以判定, 当基域 P 被扩张成为一个更大的域 Ω 时, 这个不可约表示将会按何种方式分解. 在这样一个扩张之下 Δ 变成一个代数 $\Delta_\Omega = \Delta \times \Omega$, 而左理想 $\mathfrak{l} = c_{11}\Delta + \cdots + c_{n1}\Delta$ 变成

$$\mathfrak{l}_\Omega = c_{11}\Delta_\Omega + \cdots + c_{n1}\Delta_\Omega.$$

如果 Δ_Ω 是可约的, 即 Δ_Ω 具有一个真左理想 $\mathfrak{l}'$, 那么 $\mathfrak{l}_\Omega$ 也有一个真子理想

$$\mathfrak{L}' = c_{11}\mathfrak{l}' + \cdots + c_{n1}\mathfrak{l}'.$$

同样, 如果 Δ_Ω 分解成为一些左理想 $\mathfrak{l}'$ 的直和, 那么 $\mathfrak{l}_\Omega$ 也分解成同样多个左理想的直和. 因此, 当 P 被扩张成 Ω 时, 由 $\mathfrak{l}$ 所给出的不可约表示的可约性与可分解性由代数 Δ_Ω 的可约性与分解成左理想直和的可能性所完全确定.

如果 $\Delta \neq P$, 那么根据 13.12 节, 总可以找到一个域 Ω, 使得 Δ_Ω 含有零因子, 即使得 Δ_Ω 不再是可除代数, 因而至少含有一个真左理想. 在这样的场合之下, 由 $\mathfrak{l}$ 所给出的, 在 P 中为不可约表示, 在 Ω 中便成为可约的了. 与此相反, 在 $\Delta = P$ 的情形下由 $\mathfrak{l}$ 所给出的表示是绝对不可约的, 即在基域的任意扩张之下永远保持不可约性. 因此, $\Delta = P$乃是 P 中一个不可约表示为绝对不可约的充分必要条件.

如果代数 $\mathfrak{o}$ 不是单代数, 而仅是半单的, 即 $\mathfrak{o}$ 为一些单代数的直和 $\mathfrak{a}_1+\cdots+\mathfrak{a}_s$, 并设 $\mathfrak{l}$ 是其中一个 $\mathfrak{a}_\nu$ 中的左理想, 那么为了得出 $\mathfrak{o}$ 中一个元素 a 在由 $\mathfrak{l}$ 所给出的表示之下的方阵, 首先应将 a 表成和 $a_1+\cdots+a_s$ 的形式, 在这个和中突出分量 a_ν, 然后按照公式 (14.5) 作出这个 a_ν 的表示方阵. 事实上, 其余各个分量均将理想 $\mathfrak{l}$ 零化, 因而均被映成零.

设 $\mathfrak{a}_1, \cdots, \mathfrak{a}_s$ 为可除代数 $\Delta_1, \cdots, \Delta_s$ 上的 $n_1, \cdots, n_s$ 阶全阵环, 并且 Δ_ν 的秩为 r_ν, 而 $\mathfrak{D}_\nu$ 为由 $\mathfrak{a}_\nu$ 中一个左理想 $\mathfrak{l}$ 所给出的不可约表示. 这时 $\mathfrak{o}$ 和秩 h 等于 $\mathfrak{a}_1, \cdots, \mathfrak{a}_s$ 的秩之和, 即

$$h = \sum_1^s n_\nu^2 r_\nu. \tag{14.6}$$

其次, 由 (14.5) 可以看出表示 $\mathfrak{D}_\nu$ 的级是

$$g_\nu = n_\nu r_\nu. \tag{14.7}$$

最后, $\mathfrak{a}_\nu$ 分解成 n_ν 个彼此等价的左理想 $\mathfrak{l}$ 的直和, 因此, 不可约表示 $\mathfrak{D}_\nu$ 作为正则表示的组成部分来说, 在后者中恰出现 n_ν 次.

特别, 如果所有 $\mathfrak{D}_\nu$ 都是绝对不可约的, 那么所有 $r_\nu = 1$, 因而 (14.6) 和 (14.7) 简化成

$$h = \sum_1^s n_\nu^2, \quad g_\nu = n_\nu. \tag{14.8}$$

14.3 中心的表示

在代数 $\mathfrak{o}$ 的一个不可约表示之下, 它的中心元素被映成那样一些方阵, 它们当中的每一个和一切表示方阵可交换. 如果基域是代数封闭的, 则表示方阵所组成的环为全阵环, 它的中心只能由单位方阵 E 的常数倍组成, 因此 $\mathfrak{o}$ 的中心元素被映成形为 $E\alpha$ 的方阵. 这一事实一般地对任意绝对不可约表示成立, 因为在这样的情况下, 我们可由原有的基域过渡到一个代数封闭的基域去, 而不致影响表示的不可约性. 因此, 在代数 $\mathfrak{o}$ 的一个绝对不可约表示之下, 中心元素被映成单位方阵的常数倍.

如果 $\mathfrak{o}$ 本身是可交换的, 即 $\mathfrak{o}$ 等于自己的中心, 那么一个绝对不可约表示的一切表示方阵均具有形状 $E_n\lambda$. 这时由表示的不可约性可以推出, 表示的级数应等于 1. 因此, 一个交换代数的绝对不可约表示是一级表示.

$\mathfrak{o}$ 的一个一级表示就是 $\mathfrak{o}$ 到表示域 K 内的一个同态映射. 由于 K 的交换性, 两个彼此等价的一级表示是完全相同的. 事实上, 如果 $A=(\alpha)$ 是一个表示方阵, 而 λ 为 K 中一个元素, 则

$$(\lambda)^{-1}(\alpha)(\lambda)=(\lambda^{-1}\alpha\lambda)=(\alpha).$$

由此即知, 交换代数 $\mathfrak{o}$ 在域 K 中的互不等价的一级表示的个数, 等于 $\mathfrak{o}$ 到 K 内的不相同的同态映射的个数.

现在让我们再回到非交换代数 $\mathfrak{o}$ 上去, 并设 $\mathfrak{o}$ 是半单的. 这时 $\mathfrak{o}$ 是一些单代数的直和:

$$\mathfrak{o}=\mathfrak{a}_1+\cdots+\mathfrak{a}_s,$$

而 $\mathfrak{o}$ 的中心 $\mathfrak{Z}$ 是同样多个域的直和

$$\mathfrak{Z}=\mathfrak{Z}_1+\cdots+\mathfrak{Z}_s\quad(\mathfrak{Z}_\nu\text{是}\mathfrak{a}_\nu\text{的中心}).$$

$\mathfrak{o}$ 以及 $\mathfrak{Z}$ 的互不等价的不可约表示的个数等于 $\mathfrak{o}$ 或 $\mathfrak{Z}$ 的双边分量的个数 s, 因为 $\mathfrak{o}$ 的每个这样的表示 $\mathfrak{D}_\nu$ 都由 $\mathfrak{a}_\nu$ 的一个极小左理想给出, 而 $\mathfrak{Z}$ 的每个这样的表示 $\mathfrak{D}_\nu$ 都由一个 $\mathfrak{Z}_\nu$ 给出, 因此, $\mathfrak{o}$和 $\mathfrak{Z}$ 的互不等价的不可约表示的个数相同, 并且对于 $\mathfrak{o}$ 的每个不可约表示 $\mathfrak{D}_\nu$, 如果它除 $\mathfrak{a}_\nu$ 之外, 把所有 $\mathfrak{a}_1\cdots\mathfrak{a}_s$ 均映成零的话, 我们可以使 $\mathfrak{Z}$ 的一个表示 $\mathfrak{D}'_\nu$ 与之相对应, 而后者除 $\mathfrak{Z}_\nu$ 之外, 把所有 $\mathfrak{Z}_1\cdots\mathfrak{Z}_s$ 均映成零.

特别, 如果 $\mathfrak{o}$ 是 P 上一些全阵环的直和, 那么域 $\mathfrak{Z}_\nu$ 的秩为 1, 因而同构于 P. 在这一情况下, $\mathfrak{o}$ 的不可约表示的个数 s 等于中心 $\mathfrak{Z}$ 的秩. $\mathfrak{o}$ 的不可约表示 $\mathfrak{D}_\nu$ 和

$\mathfrak{Z}$ 的不可约 (一级) 表示之间的关系这时特别简单. 在表示 $\mathfrak{D}_\nu$ 之下每个中心元素 z 被映成形如 $E\alpha$ 的方阵, 其中 E 为 n_ν 阶单位方阵. 因此 (对于固定的 ν 来说), 相应于每个 z 有一个完全确定的 α, 我们可以写

$$\alpha = \Theta_\nu(z).$$

函数 Θ_ν 给出中心的一个同态, 即有

$$\Theta_\nu(y+z) = \Theta_\nu(y) + \Theta_\nu(z),$$
$$\Theta_\nu(yz) = \Theta_\nu(y)\Theta_\nu(z),$$
$$\Theta_\nu(z\beta) = \Theta_\nu(z)\beta.$$

在这一同态之下, 除 $\mathfrak{Z}_\nu$ 之外所有 $\mathfrak{Z}_1, \cdots, \mathfrak{Z}_s$ 均被映成零. 也就是说, 同态 Θ_ν 就是早先记成 $\mathfrak{D}'_\nu$ 的中心的一级表示.

只要知道模 $\mathfrak{Z}_\nu$ 的一个 P 基, 表示 Θ_ν 也就随之确定. 我们可以取域 $\mathfrak{Z}_\nu$ 的单位元作为这样一个 P 基. 如果将 $\mathfrak{Z}$ 中的元素写成

$$z = \sum_{\nu=1}^{s} e_\nu \beta_\nu \tag{14.9}$$

的形状, 则

$$ze_\nu = e_\nu^2\beta_\nu = e_\nu\beta_\nu,$$

因此 $E\beta_\nu$ 就是表示方阵, 即有

$$\Theta_\nu(z) = \beta_\nu.$$

这样一来, (14.9) 也可以写成

$$z = \sum_{\nu=1}^{s} e_\nu \Theta_\nu(z). \tag{14.10}$$

用文字表述出来, 这就是说, 当我们将中心元素 z 按中心中的幂等元 e_ν 展开时, 展开系数 $\Theta_\nu(z)$ 就给出中心的同态或一级表示.

习题 14.1　一个交换代数 $\mathfrak{o}$ 在基域 P 的代数封闭扩域 Ω 中的一级表示的个数, 等于 $\mathfrak{o}_\Omega/\mathfrak{R}$ 在 P 上的秩, 其中 $\mathfrak{R}$ 为 $\mathfrak{o}_\Omega$ 的根.

习题 14.2　设 K 是 P 的有限扩域, 则 K 在 Ω 中的一级表示的个数等于 K 在 P 上的简约次数. $\mathfrak{R} = \{0\}$ 当且仅当 K 在 P 上为可分.

14.4　迹与特征标

元素 a 在表示 $\mathfrak{D}$ 下的迹, 写作

$$S_{\mathfrak{D}}(a) \text{ 或简写作 } S(a),$$

指的就是 a 在 $\mathfrak{D}$ 下的表示方阵 A 的迹 $S(A)$. 当 $\mathfrak{D}$ 固定时, 迹 $S_{\mathfrak{D}}$ 作为元素 a 的一个函数来看, 称为表示 $\mathfrak{D}$ 的迹.

由关系式

$$S(P^{-1}AP) = S(A)$$

可知, 等价表示有相同的迹.

迹是一个线性函数, 也就是说,

$$S(a+b) = S(a) + S(b),$$
$$S(a\beta) = S(a)\beta.$$

一个绝对不可约表示的迹 (或者, 换一个效果完全相同的说法, 代数闭域 Ω 中不可约表示的迹), 称为特征标[①]. 一个元素 a 在第 ν 个不可约表示 $\mathfrak{D}_\nu$ 下的特征标记作

$$\chi_\nu(a).$$

当我们所讨论的是某一固定的表示时, 足数 ν 迹可略去不写.

根据 14.3 节, 在一个 n_ν 级的绝对不可约表示 $\mathfrak{D}_\nu$ 之下, 中心元素 z 被映成对角形方阵 $E \cdot \Theta_\nu(z)$, 其中 $\Theta_\nu(z)$ 为中心到域 Ω 内的一个同态. 方阵 $E \cdot \Theta_\nu(z)$ 的迹是

$$\chi_\nu(z) = n_\nu \cdot \Theta_\nu(z). \tag{14.11}$$

特别, $\mathfrak{o}$ 的单位元将被映成单位方阵 E, 它的迹等于 n_ν:

$$\chi_\nu(1) = n_\nu.$$

在下面我们假定, 绝对不可约表示 $\mathfrak{D}_\nu$ 的级 n_ν 不能被域 Ω 的特征整除. 这时被 (14.11) 除以 n_ν 即得

$$\Theta_\nu(z) = \frac{\chi_\nu(z)}{n_\nu}. \tag{14.12}$$

---

① 许多作者将特征标一词也用之于可约表示, 并使用"复合特征标"这样的说法. 我们避免了这样的术语, 因为这一说法在 Abel 群的特殊情况下, 和老早就已流行的"特征标"一词的意义并不一致. 另一方面, "迹"这个词同样也能充分地表达我们所要表达的东西.

这样, 中心的同态就通过特征标表达出来了.

定理 代数 $\mathfrak{o}$ 在特征为 0 的域 Ω 中的一个完全可约表示, 在等价的意义之下由表示方阵的迹所唯一确定.

证 设 $\mathfrak{R}$ 为 $\mathfrak{o}$ 的根, 那么 $\mathfrak{o}$ 的每个完全可约表示同时也是 $\mathfrak{o}/\mathfrak{R}$ 的完全可约表示. 根据假设, 对应于 $\mathfrak{o}/\mathfrak{R}$ 中元素的那些方阵的迹是已知的. 设

$$\mathfrak{o}/\mathfrak{R} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n,$$

并设 $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ 的单位元为 $e_1, \cdots, e_n$, 那么在不可约表示 $\mathfrak{D}_\nu$ 之下元素 e_ν 将被映成 n_ν 阶单位方阵. 因此相应的迹等于

$$S_\nu(e_\nu) = n_\nu,$$

而

$$S_\nu(e_\mu) = 0, \quad 对 \quad \mu \neq \nu.$$

另一方面, 对于一个完全可约表示来说, 如果我们知道每个不可约表示 $\mathfrak{D}_\nu$ 在它里面出现多少次, 那么这个完全可约表示也就完全确定了. 不妨设表示 $\mathfrak{D}_\nu$ 出现 q_ν 次, 那么我们所考虑的完全可约表示将由 q_1 个小块 $\mathfrak{D}_1$, q_2 个小块 $\mathfrak{D}_2$ 等组成. e_ν 在这一表示中的迹等于

$$S(e_\nu) = q_\nu n_\nu. \tag{14.13}$$

只要知道了所有的迹 $S(e_\nu)$, 由 (14.13) 式就可以计算出 q_ν. 这就证明了我们的定理.

注 只要知道 $\mathfrak{o}$ 的基元素的迹, $\mathfrak{o}$ 中每个元素的迹也就完全知道了. 因此, 举例来说, 如果 $\mathfrak{o}$ 是一个有限群的群环, 那么只要知道每个群元素的迹, 表示就已确定. 设 $a_1, \cdots, a_n$ 为基元素, 而 $\chi_\nu(a_i)$ 为不可约表示的迹, 那么对任意表示来说, 有

$$S(a_i) = \sum_{\nu=1}^{s} q_\nu \chi_\nu(a_i). \tag{14.14}$$

根据上面的定理, 整数 q_ν 由这一组方程所唯一确定. 方程组 (14.14) 还提供了一个具体的计算方法, 以便完全通过迹的计算将一个完全可约表示分解成为其不可约组成部分. 当然, 首先必须知道所有不可约表示的迹.

14.5 有限群的表示

我们首先证明

Maschke 定理 设域 P 的特征不能整除有限群 $\mathfrak{G}$ 的阶 h, 则 $\mathfrak{G}$ 在 P 中的每个表示都是完全可约的.

证 设表示模 $\mathfrak{N}$ 是可约的, 并设 $\mathfrak{N}$ 为一极小子模. 我们要证明, $\mathfrak{M}$ 可表成直和 $\mathfrak{N}+\mathfrak{N}''$ 的形式, 其中 $\mathfrak{N}''$ 仍为一表示模.

作为向量空间来看, $\mathfrak{M}$ 有形如 $\mathfrak{N}+\mathfrak{N}'$ 的分解, 可是这里的 $\mathfrak{N}'$ 还不一定在 $\mathfrak{o}$ 下不变. 设 y 为 $\mathfrak{N}'$ 中的一个元素, a 为 $\mathfrak{G}$ 中一个元素, 则 ay 可唯一地表成 $\mathfrak{N}$ 中一个元素和 $\mathfrak{N}'$ 中一个元素 y' 之和, 因此

$$ay \equiv y'(\mathrm{mod}\ \mathfrak{N}).$$

对于固定的 a, 元素 y' 由 y 所唯一确定, 并且线性地依赖于 y: 由 $ay \equiv y'$ 和 $az \equiv z'$ 可推出 $a(y+z) \equiv y'+z'$ 和 $a(y\beta) \equiv y'\beta$ $(\beta \in P)$. 因此我们可以写

$$y' = A'y; \quad A'y \equiv ay(\mathrm{mod}\ \mathfrak{N}),$$

其中 A' 为 $\mathfrak{N}'$ 内的一个线性变换, 它是由 a 决定的. 不但如此, 线性变换 A' 甚至还是 $\mathfrak{G}$ 的一个表示, 因为由 $a \to A'$ 和 $b \to B'$ 可推得 $ab \to A'B'$.

如果命

$$\frac{1}{h}\sum_a a^{-1}A'y = Qy = y'',$$

则 y'' 线性地依赖于 y, 因而 y'' 组成一个线性子空间 $\mathfrak{N}'' = Q\mathfrak{N}'$. 其次, 相对于模 $\mathfrak{N}$ 来看, 我们有同余关系:

$$y'' \equiv \frac{1}{h}\sum_a a^{-1}ay = y.$$

因此, $\mathfrak{M}$ 中的每个元素 mod $\mathfrak{N}$ 不但同余于 $\mathfrak{N}'$ 中的一个元素 y', 而且同余于 $\mathfrak{N}''$ 中的一个元素 y''. 这就是说, 我们有直分解

$$\mathfrak{M} = \mathfrak{N} + \mathfrak{N}''.$$

最后, 对 $\mathfrak{G}$ 中每个元素 b, 有

$$\begin{aligned} by'' &= \frac{1}{h}\sum_a ba^{-1}A'y \\ &= \frac{1}{h}\sum_a (ab^{-1})^{-1}(A'B'^{-1})B'y \\ &= QB'y \in Q\mathfrak{N}' = \mathfrak{N}''. \end{aligned}$$

因此 $\mathfrak{N}''$ 被 $\mathfrak{G}$ 中的算子 b 映成其自身, 即 $\mathfrak{N}''$ 为一表示模.

如果 $\mathfrak{N}''$ 仍是可约的, 那么我们又可以用同样方式处理 $\mathfrak{N}''$, 从而再分解出一个极小子模来. 余此类推. 最后可得出模 $\mathfrak{M}$ 亦即得出表示的一个完全分解. Maschke 定理获证.

根据 14.1 节, 群 $\mathfrak{G}$ 的每个表示可开拓成群环

$$\mathfrak{o} = a_1 P + \cdots + a_h P$$

的一个表示. 反之, $\mathfrak{o}$ 的每个表示自然诱导出 $\mathfrak{G}$ 的一个表示. 由 Maschke 定理可知, $\mathfrak{o}$ 的每个表示是完全可约的. 特别, $\mathfrak{o}$ 的正则表示, 即以 $\mathfrak{o}$ 自身作为表示模的表示是完全可约的. 因此 $\mathfrak{o}$ 是一些极小左理想的直和, 从而据 13.7 节定理 13, $\mathfrak{o}$ 是半单的. 根据 14.2 节, $\mathfrak{o}$ 的极小左理想给出一切可能的不可约表示.

根据 14.3 节, 绝对不可约表示的个数等于中心的秩. 不难看出, 群环的中心由所有这样的和

$$\sum_{\lambda} a_{\lambda}\beta_{\lambda} \tag{14.15}$$

组成, 其中共轭的群元素具有相同的系数. 与元素 a 共轭的元素组成一个共轭"类". 如果命 k_a 表示这个共轭类中各个元素之和, 则 (14.15) 就是这样一些 k_a 的一个线性组合, 其系数属于 P. 因此我们有下面的定理: *群环的中心由类和 k_a 张成*. 这样一来, 中心的秩等于共轭类的个数, 由此即得

一个群的互不等价的绝对不可约表示的个数等于这个群中共轭元素类的个数.

根据 14.2 节, 这些绝对不可约表示的级数 $n_1, \cdots, n_s$ 之间存在着关系

$$n_1^2 + n_2^2 + \cdots + n_s^2 = h.$$

一个永远存在的一级表示就是群的"单位表示", 它把每个群元素都映成 1. 如果还有其他的一级表示, 那么群中必存在具有 Abel 商群的正规真子群, 因为一个一级表示的表示方阵是彼此可交换的, 它们组成一个和原来的群同态的 Abel 群. 反之, 如果群中存在一个正规真子群, 其商群为 Abel 群, 那么这一商群的特征标就给出原有群的一级表示. 所有其余的表示都是高级的.

例 1　*对称群 $\mathfrak{S}_3$*. 共轭类数等于 3, 因此有 3 个表示. 交错群有两个陪集 $\mathfrak{K}_0$ 和 $\mathfrak{K}_1$, 即偶置换所成的陪集与奇置换所成的陪集. 这个二元群的两个特征标是

$$\chi(\mathfrak{K}_0) = 1, \quad \chi(\mathfrak{K}_1) = \pm 1.$$

它们给出 $\mathfrak{S}_3$ 的全部一级表示. 由于

$$n_1^2 + n_2^2 + n_3^2 = 6,$$

第三个表示的级数应为 2. 在平面上取三个向量 e_1, e_2, e_3, 使其和为零. 这三个向量之间的置换给出 $\mathfrak{S}_3$ 的一个忠实的表示. 如果取 e_1 和 e_2 为基本向量, 则表示的形式为

$$\begin{cases}(1\ 2)e_1 = e_2, \\ (1\ 2)e_2 = e_1\end{cases} \qquad \begin{cases}(1\ 3)e_1 = -e_1 - e_2, \\ (1\ 3)e_2 = e_2,\end{cases} \qquad \begin{cases}(2\ 3)e_1 = e_1, \\ (2\ 3)e_2 = -e_1 - e_2,\end{cases}$$

$$\begin{cases}(1\ 2\ 3)e_1 = e_2, \\ (1\ 2\ 3)e_2 = -e_1 - e_2,\end{cases} \qquad \begin{cases}(1\ 3\ 2)e_1 = -e_1 - e_2, \\ (1\ 3\ 2)e_2 = e_1.\end{cases}$$

例 2 四元数群 $\mathfrak{Q}_8$ 就是八个四元数 $\pm 1, \pm 1, \pm k, \pm l$ 所组成的群. 它有两个生成元 i 和 k, 二者满足关系

$$j^4 = 1, \quad k^2 = j^2, \quad kj = j^3 k.$$

共轭类数是 5, 因此有 5 个表示. 正规子群 $\{1, j^2\}$ 的商群为 Klein 四元群, 后者的 4 个特征标即给出 $\mathfrak{Q}_8$ 的 4 个一级表示. 由于

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 8,$$

剩下的一个表示的级数应为 2. 如果命群元素 $1, j, j^2, j^3, k, jk, j^2k, j^3k$ 与四元数 $1, j, -1, -j, k, l, -k, -l$ 相对应, 则得到群环 $\mathfrak{o}$ 到四元数体之上的一个同态映射. 因此, 四元数体应是 $\mathfrak{o}$ 的双边合成因子之一. 这样一来, 我们就已经在有理数域 $\mathbb{Q}$ 的范围之内得出了 $\mathfrak{o}$ 的分解, 即

$$\mathfrak{o} = \mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 + \mathfrak{a}_4 + \mathfrak{a}_5,$$

其中 $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4$ 同构于 $\mathbb{Q}$, 而 $\mathfrak{a}_5$ 同构于 $\mathbb{Q}$ 上的四元数体. 过渡到一个代数封闭的基域去 (在目前情况下, 实际只要添加 $\mathrm{i} = \sqrt{-1}$ 就够了), 则四元数体受到分裂, 从而得出方阵表示

$$j \to \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \quad k \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad l \to \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}.$$

例 3 交错群 $\mathfrak{A}_4$. 可以用处理对称群 $\mathfrak{S}_3$ 的同一方法来处理, 这一工作我们留给读者去作. 可以找出 $\mathfrak{A}_4$ 的四个表示, 其级数为 1, 1, 1, 3.

例 4 对称群 $\mathfrak{S}_4$. 共轭类数为 5, 因此有 5 个表示. Klein 四元群 $\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ 的商群同构于 $\mathfrak{S}_3$, 我们已经得出了 $\mathfrak{S}_3$ 的 3 个不可约表示, 其级数为 1, 1, 2. 这三个表示也就给出 $\mathfrak{S}_4$ 的三个级为 1, 1, 2 的表示. 如记这三个级数为 n_1, n_2, n_3, 则有

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 24,$$

从而有

$$n_4^2 + n_5^2 = 18,$$

这只有当 $n_4 = 3, n_5 = 3$ 时才可能成立. 在三维空间中取 4 个向量 e_1, e_2, e_3, e_4, 使得其和为零. 这四个向量的置换给出群 $\mathfrak{S}_4$ 的一个忠实的三级表示.

如命 e_1, e_2, e_3 为基本向量, 则表示的形式为

$$\begin{cases} (1\ 2)e_1 = e_2, \\ (1\ 2)e_2 = e_1, \\ (1\ 2)e_3 = e_3, \end{cases} \quad \begin{cases} (1\ 3)e_1 = e_3, \\ (1\ 3)e_2 = e_2, \\ (1\ 3)e_3 = e_1, \end{cases} \quad \begin{cases} (1\ 4)e_1 = -e_1 - e_2 - e_3, \\ (1\ 4)e_2 = e_2, \\ (1\ 4)e_3 = e_3, \end{cases}$$

$$\begin{cases} (1\ 2\ 3)e_1 = e_2, \\ (1\ 2\ 3)e_2 = e_3, \\ (1\ 2\ 3)e_3 = e_1, \end{cases} \qquad \text{余类此.}$$

由于这个表示是忠实的, 故不可能把它分解成一级和二级表示, 因此它是一个不可约表示. 将所有奇置换的表示方阵乘以 -1, 就得另一个忠实的, 从而也是不可约的三级表示. 这个新的三级表示一定不会和前一表示等价, 因为二者的迹不相同. 这样我们就把一切表示找出来了.

习题 14.3　群环 $\mathfrak{o}$ 中的元素 $s = \sum\limits_{a \in \mathfrak{G}} a$ 满足方程

$$bs = s, \qquad \text{对} b \in \mathfrak{G}.$$

s 生成怎样的左理想? 这个左理想给出怎样的表示? 这个理想中包含着怎样的幂等元?

习题 14.4　如果群元素的个数 h 能被域的特征整除, 则习题 14.3 中的理想是幂零的. 由此推出, 特征不能整除 h 这一条件对 Maschke 定理来说是必要的.

14.6　群 特 征 标 [①]

线性变换的 Kronecker 积

假设给定了两个线性变换 A' 和 A'', 其中一个作用在向量空间 $(u_1, \cdots, u_m)$ 之内, 另一个作用在向量空间 $(v_1, \cdots, v_m)$ 之内:

$$A'u_k = \sum_i u_i \alpha'_{ik},$$

① 文献：关于有限群表示理论的一个不以超复系理论为基础的叙述，可参看 Schur I. *Neue Begründung der Theorie der Gruppencharaktere.* Sitzungsber, Berlin, 1905: 406. 这一理论对无限群的推广见 Neumann J V. Almost periodic functions in groups. *Trans. Amer. Math. Soc.*, 1934, 36. 关于进一步的文献可参看 van der Waerden B L. Gruppen von linearen Transformationen. *Ergebn. Math.,* IV 2. Berlin, 1935.

$$A''v_l = \sum_j v_j \alpha''_{jl}.$$

我们按 13.3 节中所述方式, 由这两个向量空间作积空间, 后者由积 $u_k v_l$ 张成. 定义

$$A(u_k v_l) = (A'u_k)(A''v_l) = \sum_i \sum_j u_i v_j \alpha'_{ik} a''_{jl}. \tag{14.16}$$

这样定义出来的积空间内的线性变换 A 称为 A' 和 A'' 的 Kronecker积变换, 并记作 $A' \times A''$. 由 (14.16) 可以看出, A 的方阵系数是 $\alpha'_{ik}\alpha''_{jl}$. A 的迹等于

$$\sum_i \sum_j \alpha'_{ii}\alpha''_{jj} = \sum_i \alpha'_{ii} \cdot \sum_j \alpha'_{jj} = S(A') \cdot S(A'').$$

因此, 积变换 $A' \times A''$ 的迹等于变换 A' 和 A'' 的迹的乘积.

如果对向量 u 相继作两次线性变换 B', A', 对向量 v 相继作两次线性变换 B'', A'', 则积 $u_k v_l$ 依次受到变换 $B' \times B''$ 和 $A' \times A''$ 的作用. 这就是说

$$(A' \times A'') \cdot (B' \times B'') = A'B' \times A''B''. \tag{14.17}$$

如果方阵 $A', B', \cdots$ 构成 $\mathfrak{G}$ 的一个表示 $\mathfrak{D}'$, 方阵 $A'', B'', \cdots$ 构成 $\mathfrak{G}$ 的另一表示 $\mathfrak{D}''$, 则由 (14.17) 可以看出, 积变换 $A = A' \times A'', B = B' \times B'', \cdots$ 仍构成一个表示. 表示 $\mathfrak{D}'$ 和 $\mathfrak{D}''$ 的这个积表示记作 $\mathfrak{D}' \times \mathfrak{D}''$.

再命 $\mathfrak{D}' + \mathfrak{D}''$ 代表一个能够分解成 $\mathfrak{D}'$ 和 $\mathfrak{D}''$ 的可约表示, 并将彼此等价的表示看成相同, 那么容易验证下列运算规则成立：

$$\begin{aligned}
&\mathfrak{D}' + \mathfrak{D}'' = \mathfrak{D}'' + \mathfrak{D}', \mathfrak{D}' \times \mathfrak{D}'' = \mathfrak{D}'' \times \mathfrak{D}',\\
&\mathfrak{D}' + (\mathfrak{D}'' + \mathfrak{D}''') = (\mathfrak{D}' + \mathfrak{D}'') + \mathfrak{D}''',\\
&\mathfrak{D}' \times (\mathfrak{D}'' \times \mathfrak{D}''') = (\mathfrak{D}' \times \mathfrak{D}'') \times \mathfrak{D}''',\\
&\mathfrak{D}' \times (\mathfrak{D}'' + \mathfrak{D}''') = \mathfrak{D}' \times \mathfrak{D}'' + \mathfrak{D}' \times \mathfrak{D}''',\\
&(\mathfrak{D}'' + \mathfrak{D}''') \times \mathfrak{D}' = \mathfrak{D}'' \times \mathfrak{D}' + \mathfrak{D}''' \times \mathfrak{D}'.
\end{aligned}$$

特别, 如果 $\mathfrak{G}$ 是一个有限群, 其阶不能被域 P 的特征整除, 那么每个表示都完全分解成不可约表示 $\mathfrak{D}_\nu$, 从而有

$$\mathfrak{D}_\lambda \times \mathfrak{D}_\mu = \sum_\nu c^\nu_{\lambda\mu} \mathfrak{D}_\nu, \tag{14.18}$$

其中 $c^\nu_{\lambda\mu}$ 为非负整数. 在 (14.18) 中 ν 并非幂指数, 而是一个标号.

对迹来说, 由 (14.18) 可以推出

$$S_\lambda(a) \cdot S_\mu(a) = \sum_\nu c^\nu_{\lambda\mu} S_\nu(a).$$

如果所考虑的不可约表示是绝对不可约的, 从而迹即为特征标, 那么我们可以把这个式子写成

$$\chi_\lambda(a)\cdot\chi_\mu(a)=\sum_\nu c^\nu_{\lambda\mu}\chi_\nu(a) \quad (\text{第一特征标关系}). \tag{14.19}$$

作为类函数的特征标

设 a 和 a' 为共轭的群元素:

$$a'=bab^{-1},$$

那么对表示方阵来说, 将有

$$A'=BAB^{-1}.$$

因此 A 和 A' 有相同的迹, 亦即

$$S(bab^{-1})=S(a),$$

特别

$$\chi(bab^{-1})=\chi(a).$$

如果把所有和 a 共轭的元素归为一类 $\mathfrak{K}_a$, 那么每个特征标对同一类 $\mathfrak{K}_a$ 中的各个元素的值相同.

如果共轭类 $\mathfrak{K}_a$ 中元素的个数为 h_a, 而各个元素之和为 k_a(属于群环 $\mathfrak{o}$), 则 k_a 的特征标等于这个共轭类中各个元素的特征标之和, 即有

$$\chi(k_a)=h_a\cdot\chi(a).$$

从现在起我们假定, 不论是群的阶 h, 或绝对不可约表示 $\mathfrak{D}_\nu$ 的级数 n_ν 都不能被基域的特征整除. 正如我们在 14.5 节中所见到过的那样, 元素 k_a 张成群环 $\mathfrak{o}$ 的中心 $\mathfrak{Z}$. 根据 14.4 节, 中心 $\mathfrak{Z}$ 的同态 Θ_ν 和特征标 χ_ν 之间有关系

$$\Theta_\nu(z)=\frac{\chi_\nu(z)}{n_\nu},$$

特别, 我们有

$$\Theta_\nu(k_a)=\frac{\chi_\nu(k_a)}{n_\nu}=\frac{h_a}{n_\nu}\chi_\nu(a). \tag{14.20}$$

乘积 k_ak_b 乃是一些群元素之和, 并且仍旧属于 $\mathfrak{Z}$, 因此它可以表成类和 k_c 的一个整系数线性组合:

$$k_a\cdot k_b=\sum_c g^c_{ab}k_c. \tag{14.21}$$

这时 Θ_ν 的同态性质表现为如下的方程：

$$\Theta_\nu(k_a)\Theta_\nu(k_b)=\sum_c g_{ab}^c\Theta_\nu(k_c), \tag{14.22}$$

利用 (14.20), 这个关系式可以写为

$$h_a h_b\chi_\nu(a)\chi_\nu(b)=n_\nu\sum_c g_{ab}^c h_c\chi_\nu(c)\quad (\text{第二特征标关系}). \tag{14.23}$$

在和 (14.21)~ (14.23) 中, c 每次都是遍历群 $\mathfrak{G}$ 的共轭类的一个代表系. 如果命 c 遍历所有群元素, 那么在 (14.23) 式右端就不必写上因子 h_c. 由于 Θ_ν 乃是 $\mathfrak{Z}$ 所仅有的几个同态, 所以 χ_ν 乃是方程 (14.23) 的仅有的几个解.

共轭特征标

每个表示 $a\to A$ 有一个共轭(或逆变) 表示 $a\to A'^{-1}$, 其中 A' 为 A 的转置方阵. 事实上, 在这一对应之下, 有

$$ab\to(AB)'^{-1}=(B'A')^{-1}=A'^{-1}B'^{-1}.$$

共轭表示的共轭表示即原来的表示. 如果表示 $a\to A$ 是可约的, 那么它的共轭表示也是可约的, 反之亦然. 因此一个不可约表示的共轭表示也是不可约的.

当由 A 过渡到等价表示 PAP^{-1} 时, A 的共轭表示将过渡到

$$(PAP^{-1})'^{-1}=P'A'^{-1}P'^{-1},$$

即亦过渡到自己的一个等价表示.

如果命 $\mathfrak{D}_{\nu'}$ 代表和 $\mathfrak{D}_\nu$ 共轭的不可约表示, 并设 $\mathfrak{D}_\nu(a)=A$, 则

$$\mathfrak{D}_{\nu'}(a^{-1})=A',$$

但 A' 的迹等于 A 的迹, 故

$$\chi_{\nu'}(a^{-1})=\chi_\nu(a).$$

我们把与 χ_ν共轭的特征标$\chi_{\nu'}$ 记作 $\overline{\chi}_\nu$.

每个特征标都是一些单位根之和. 事实上, $\mathfrak{G}$ 的每个元素 a 生成一个循环子群 $\mathfrak{C}$, 其阶 m 为 h 的一个因子. $\mathfrak{G}$ 的每个不可约表示 $\mathfrak{D}_\nu$ 诱导出 $\mathfrak{C}$ 的一个表示. 后者完全分解成一些一级表示, 其方阵系数为 m 次单位根. 表示方阵的迹是对角线元素之和, 因而是一些 m 次单位根的和, 即

$$\chi(a)=\zeta^{\nu_1}+\zeta^{\nu_2}+\cdots+\zeta^{\nu_n}, \tag{14.24}$$

其中 ζ 为一 m 次本原单位根.

其他特征标关系

设 $S(c)$ 为群元素 c 在正则表示之下的迹, 因为正则表示包含不可约表示 $\mathfrak{D}_\nu$ 恰恰 n_ν 次, 故必有

$$S(c)=\sum_\nu n_\nu\chi_\nu(c).$$

可是另一方面, 迹 $S(c)$ 是可以直接计算的: 群元素 $a_1,\cdots,a_h$ 组成正则表示空间 $\mathfrak{o}$ 的一个基, 并且

$$ca_i=a_k.$$

只有当 c 等于群中的单位元 1 时才会出现 $i=k$, 而在这一情况之下每个 i 都等于相应的 k. 因此有

$$S(1)=h,\quad S(c)=0,\quad \text{对}c\neq 1.$$

这就是说

$$\sum_\nu n_\nu\chi_\nu(c)=\begin{cases}h, & \text{对}c=1,\\ 0, & \text{对}c\neq 1.\end{cases}\tag{14.25}$$

将式 (14.23) 对一切 ν 求和, 并利用式 (14.25), 即得

$$h_ah_b\sum_\nu\chi_\nu(a)\chi_\nu(b)=g_{ab}^1h.\tag{14.26}$$

数 g_{ab}^1 说明, 有多少次从 $\mathfrak{K}_a$ 中取一元素 a', 从 $\mathfrak{K}_b$ 中取一元 b' 相乘之积 $a'b'$ 等于 1. 如果没有一对互逆的元素分别包含在 $\mathfrak{K}_a$ 和 $\mathfrak{K}_b$ 之内, 那么这个数就等于零. 如果存在这样一对元素, 譬如说 $b=a^{-1}$, 那么对 $\mathfrak{K}_a$ 中任意元素 $a'=cac^{-1}$,$\mathfrak{K}_b$ 包含着它的逆元 $b'=a'^{-1}=cbc^{-1}$, 因此有

$$g_{ab}^1=h_a=h_b.$$

这样一来, 将 (14.26) 除以 h_b 即得

$$h_a\sum_\nu\chi_\nu(a)\chi_\nu(b)=\begin{cases}h, & \text{对}\mathfrak{K}_b=\mathfrak{K}_{a^{-1}},\\ 0, & \text{对}\mathfrak{K}_b\neq\mathfrak{K}_{a^{-1}}\end{cases}\ (\text{第三特征标关系}).\tag{14.27}$$

当 $a=1$ 时, 作为一个特例可重新得出 (14.25)

现在假设 $a_1,\cdots,a_s$ 是所有共轭类的一个代表系. 命

$$\begin{aligned}\chi_{\nu\mu}&=\chi_\nu(a_\mu),\\ \eta_{\mu\nu}&=\frac{h_\mu}{h}\overline{\chi}_\nu(a_\mu)=\frac{h_\mu}{h}\chi_\nu(a_\mu^{-1}),\end{aligned}$$

关系式 (14.27) 表明方阵 $X=(\chi_{\mu\nu})$ 和 $Y=(\eta_{\mu\nu})$ 是互逆的：

$$YX=E \text{ 或 } Y=X^{-1}. \tag{14.28}$$

由 (14.28) 立得

$$XY=E,$$

具体写出来就是

$$\frac{1}{h}\sum_{\mathfrak{K}_a} h_a\chi_\nu(a)\overline{\chi}_\mu(a)=\begin{cases}1, & \text{对}\nu=\mu,\\ 0, & \text{对}\nu\neq\mu,\end{cases} \tag{14.29}$$

其中 a 遍历所有共轭类的一个代表系. 如果命 a 遍历所有群元素, 那么就必须去掉因子 h_a. 由此即得出特征标的正交性:

$$\sum_{a\in\mathfrak{G}}\overline{\chi}_\mu(a)\chi_\nu(a)=\begin{cases}h, & \text{对}\nu=\mu,\\ 0, & \text{对}\nu\neq\mu \text{ (第四特征标关系)}.\end{cases} \tag{14.30}$$

特别, 如果 $\mu=0$, 即 χ_μ 为单位表示 χ_0 的特征标, 则由 (14.30) 可得

$$\sum_a\chi_\nu(a)=\begin{cases}h, & \text{对}\nu=0,\\ 0, & \text{对}\nu\neq 0.\end{cases} \tag{14.31}$$

方阵 X 和 Y 互逆这一事实可以利用来计算幂等中心元素 $e_1,\cdots,e_s$. 这些元素生成 $\mathfrak{o}$ 中的双边单理想. 事实上, 根据 14.5 节可知, 中心 $\mathfrak{Z}$ 的基元素 k_a 有表达式

$$k_a=\sum_\nu e_\nu\Theta_\nu(k_a)=\sum_\nu e_\nu\frac{h_a}{n_\nu}\chi_\nu(a). \tag{14.32}$$

两端乘以 $\overline{\chi}_\mu(a)$ 并对一切共轭类 $\mathfrak{K}_a$ 求和, 可得

$$\sum_{\mathfrak{K}_a}k_a\overline{\chi}_\mu(a)=e_\mu\cdot\frac{h}{n_\mu},$$

或

$$e_\nu=\sum_{\mathfrak{K}_a}k_a\frac{n_\nu}{h}\chi_\nu(a^{-1}).$$

14.7 对称群的表示 ①

我们考虑 n 个文字 1, 2, $\cdots$, n 的全部置换所组成的群 $\mathfrak{S}_n$, 并设法找出这个群, 譬如说, 在全部代数数所组成的域 Ω 中的一切绝对不可约表示. 下面的研究将要表明, 这些表示都是有理的, 也就是说, 它们都可以在有理数域 $\mathbb{Q}$ 中写出来.

① 本书中所给的证明较之 Frobenius 的理论 (Sitzungsber. Berlin, 1903: 328) 已大大化简. 这个证明是 Neumann 先生口头通知作者的, 谨此致谢.

我们从群环 $\mathfrak{o}=s_1\Omega+\cdots+s_{n!}\Omega$ 出发, 并考虑它的左理想. 每个这样的左理想都是一些极小左理想的直和, 后者给出 $\mathfrak{S}_n$ 的不可约表示. 由于每个左理想都能由一个幂等元生成, 故我们首先要设法找出幂等元.

我们把文字 $1,2,\cdots,n$ 按任意顺序一行接着一行地排成 h 行 (h 也是任意的), 使得在第 ν 行中出现 α_ν 个文字, 并且条件

$$\begin{cases}\alpha_1\geqslant\alpha_2\geqslant\cdots\geqslant a_h,\\ \displaystyle\sum_{\nu=1}^{h}\alpha_\nu=n\end{cases}\tag{14.33}$$

成立. 把这 h 个行中的第一个文字一个接着一个地排成一列, 然后再把各行中的第二个文字一个接着一个地排成一列, 余此类推, 也就是把全部文字排成下面所示的图式, 其中的点代表文字：

$$\begin{array}{lll}\cdot&\cdot&\cdot\\ \cdot&\cdot&\\ \cdot&\cdot&\end{array}\qquad(\alpha_1,\alpha_2,\alpha_2)=(3,2,2),\quad n=7.$$

文字 $1,2,\cdots,n$ 的这样一种安置称为一个图式Σ_α, 足标 α 代表数列 $(\alpha_1,\alpha_2,\cdots,\alpha_h)$. 各个可能的足标 α 可按照如下的方式来编序：即 $\alpha>\beta$, 如果第一个不等于零的差 $\alpha_\nu-\beta_\nu$ 是正的. 举例来说, 当 $n=5$ 时, 有

$$5>(4,1)>(3,2)>(3,1,1)>(2,2,1)>(2,1,1,1)>(1,1,1,1,1).$$

当一个图式给定时, 我们命 p 表示所有那样的置换, 它们只在图式中每一个行之内置换各个文字, 但保持每个行不变；而用 q 表示那样的置换, 它们只在图式中每个列之内置换各个文字. 对每个 q, 命 σ_q 等于数 $+1$ 或 -1, 视 q 为奇置换或偶置换而定. 如果 s 是任意置换, 命 $s\Sigma_\alpha$ 表示图式 Σ_α 经受置换 s 的作用所得到的那个图式. 容易看出, 如果 q 使得 Σ_α 的各个列不变, 则 sqs^{-1} 使 $s\Sigma_\alpha$ 的各个列不变, 反之亦然. 最后, 对每个固定的 Σ_α(在群环 $\mathfrak{o}$ 内) 命

$$S_\alpha=\sum_p p,$$

$$A_\alpha=\sum_q q\sigma_q.$$

不难验证下面的规则成立：

$$pS_\alpha=S_{\alpha P}=S_\alpha,\tag{14.34}$$

$$A_\alpha q\sigma_q = qA_\alpha\sigma_q = A_\alpha. \tag{14.35}$$

由 (14.34) 和 (14.35) 容易推出, S_α 和 A_α 乘上一个适当的因子 f_α 之后是幂等的. S_α 和 A_α 的进一步的代数性质可由下述组合引理中推出：

设 Σ_α 和 Σ_β 是如上所述的两个图式, 并且 $\alpha \geqslant \beta$. 如果出现在 Σ_α 中同一行之内的任意两个文字在 Σ_β 中不出现于同一列之内, 那么必有 $\alpha=\beta$, 并且图式 Σ_β 可由图式 Σ_α 经过一个形为 pq 的置换的作用得出

$$pq\Sigma_\alpha = \Sigma_\beta$$

(这里记号 p 和 q 是相对于 Σ_α 来说的, 即 p 使 Σ_α 的行不变, q 使 Σ_α 的列不变).

证　由 $\alpha \geqslant \beta$ 可推出 $\alpha_1 \geqslant \beta_1$. 在 Σ_α 的第一行中有 α_1 个文字. 如果这些文字在 Σ_β 中出现于不同的列, 那么 Σ_β 至少要有 α_1 个列才行, 因此 $\alpha_1 \leqslant \beta_1$, 从而有 $\alpha_1=\beta_1$. 经过一个使 Σ_β 的列不变的置换 q_1' 之后, 可使这些文字全都出现在 Σ_β 的第一行之内.

现在由 $\alpha \geqslant \beta$ 可推出 $\alpha_2 \geqslant \beta_2$. 事实上, 在 Σ_α 的第二行中有 α_2 个文字. 如果这些文字在 $q_1'\Sigma_\beta$ 中出现于不同的列, 那么 $q_1'\Sigma_\beta$ 中除掉第一个行之后至少应有 α_2 个列, 因此这 α_2 个文字中一个也不会出现在 $q_1\Sigma_\beta$ 的第一行中. 由此即知 $\alpha_2 \leqslant \beta_2$, 从而有 $\alpha_2=\beta_2$. 经过一个使得 $q_1'\Sigma_\beta$ 的各个列以及它的第一行不变的置换 q_2' 之后, 可以使这些文字都出现在 Σ_β 的第二行之内.

如此进行下去, 可得出一个图式 $q'\Sigma_\beta = q_h'\cdots q_2'q_1'\Sigma_\beta$, 它的各行和 Σ_α 的各行所含文字相同. 因此可以用一个置换 p 将 Σ_α 变成 $q'\Sigma_\beta$：

$$q'\Sigma_\beta = p\Sigma_\alpha.$$

置换 $q'=q_h'\cdots q_2'q_1'$ 使得 Σ_β 的列不变, 因而也使得 $q'\Sigma_\beta = p\Sigma_\alpha$ 的列不变. 因此, 对适当的 q 有

$$q' = pq^{-1}p^{-1},$$

从而

$$pq^{-1}p^{-1}\Sigma_\beta = p\Sigma_\alpha,$$

$$\Sigma_\beta = pq\Sigma_\alpha.$$

证毕.

由这个组合引理首先可以推出

$$A_\beta S_\alpha = 0, \quad 如果\alpha > \beta. \tag{14.36}$$

事实上, 如果 $\alpha > \beta$, 那么由组合引理可知, 必有一对那样的文字, 它们在 Σ_α 中属于同一行而在 Σ_β 中属于同一列. 如果 t 为交换这两个文字的对换, 则由 (14.34) 和 (14.35) 立得

$$A_\beta S_\alpha = A_\beta t t^{-1} S_\alpha = -A_\beta S_\alpha,$$

由此即得 (14.36)

同样可证

$$S_\alpha A_\beta = 0, \quad \text{如果}\alpha > \beta.$$

此外, 由 A_β 经任意置换 s 变形所得的元素也应被 S_α 所零化:

$$S_\alpha s A_\beta s^{-1} = 0, \quad \text{如果}\alpha > \beta$$

因为 $sA_\beta s^{-1}$ 仍旧是一个 A_β, 只不过它是属于变换了的图式 $s\Sigma_\alpha$ 而已. 将上式右乘 $s\Omega$ 并对 $\mathfrak{S}_n$ 中一切 s 求和, 即有

$$S_\alpha \Big(\sum s\Omega\Big) A_\beta = (0),$$

或

$$S_\alpha \mathfrak{o} A_\beta = (0) \quad (\alpha > \beta). \tag{14.37}$$

这就是说, 当 $\beta < \alpha$ 时左理想 $\mathfrak{o}A_\beta$ 被 S_α 所零化, 或者说, 在由 $\mathfrak{o}A_\beta$ 所给出的表示之下, S_α 被映成零, 与此相反, $S_\alpha A_\alpha \neq 0$, 因为在乘积 $S_\alpha A_\alpha$ 中单位元的系数不等于零. 这就是说, 在由 $\mathfrak{o}A_\alpha$ 所给出的表示之下 S_α 不被映成零. 因此, 这个表示至少应包含一个不出现在任何 $\mathfrak{o}A_\beta(\beta < \alpha)$ 之内的不可约组成部分. 下面我们要确定这样一些不可约组成部分.

根据 (14.34) 和 (14.35), 元素 $S_\alpha A_\alpha = \sum\limits_p \sum\limits_q pq\sigma_q$ 具有性质

$$pS_\alpha A_\alpha q\sigma_q = S_\alpha A_\alpha.$$

现在我们证明, $S_\alpha A_\alpha$ 除了相差一个常数因子之外乃是群环中具有这一性质的唯一元素. 我们证明：群环 $\mathfrak{o}$ 中一个具有性质：

$$paq\sigma_q = a \quad (\text{对一切 } p, q) \tag{14.38}$$

的元素 a, 必具有形式 $(S_\alpha A_\alpha)\cdot\gamma$.

证　设

$$a = \sum_s s\gamma_s \quad (\gamma_s \in \Omega). \tag{14.39}$$

以 (14.39) 代入 (14.38) 可得

$$\sum_s s\gamma_s = \sum_s psq\sigma_q\gamma_s, \tag{14.40}$$

左端只有一个带 pq 的项, 即 $pq\gamma_{pq}$, 右端也只有一个这样的项, 即相当于 $s=1$ 的那一项. 比较系数是

$$\gamma_{pq} = \sigma_q\gamma_1.$$

现在我们取出一个不能表成 pq 这种形式的 s 来. 这时 $s\Sigma_\alpha$ 不同于一切 $pq\Sigma_\alpha$, 因而根据组合引理必可找到两个文字 i 和 k, 它们在 Σ_α 中属于同一行, 而在 $s\Sigma_\alpha$ 中属于同一列. 如果命 t 表示这两个文字的对换: $t=(jk)$, 则 $t'=s^{-1}ts$ 只交换文字 $s^{-1}j, s^{-1}k$, 而这两个文字在 $s^{-1}s\Sigma_\alpha = \Sigma_\alpha$ 中是属于同一列的. 因此 t 是一个置换 p, 而 t' 是一个置换 q, 因而在 (14.40) 中可以命 $p=t, q=t'$. 这样一来, 对我们所取的这个 s 来说, 就有

$$psq = tss^{-1}ts = s,$$
$$\sigma_q = -1.$$

比较 (14.40) 式中两端 s 的系数, 就得

$$\gamma_s = -\gamma_s, \quad \gamma_s = 0.$$

由此可见, (14.39) 式中只出现 $s=pq$ 的项, 其系数为 $\gamma_s = \sigma_q\gamma_1$, 亦即

$$a = \sum_{p,q} pq\sigma_q\gamma_1 = (S_\alpha A_\alpha)\gamma_1.$$

证毕.

由以上所证立即可以推出, 对 $\mathfrak{o}$ 中任意元素 b, 元素 $S_\alpha bA_\alpha$ 具有形式 $(S_\alpha A_\alpha)\gamma$, 因为对任意 p 和 q, 有

$$pS_\alpha bA_\alpha q\sigma_q = S_\alpha bA_\alpha.$$

因此有

$$S_\alpha\mathfrak{o}A_\alpha \subseteq (S_\alpha A_\alpha)\Omega.$$

命 $S_\alpha A_\alpha = I_\alpha$, 则有

$$I_\alpha\mathfrak{o}I_\alpha \subseteq S_\alpha\mathfrak{o}A_\alpha \subseteq I_\alpha\Omega. \tag{14.41}$$

现在我们断定, $\mathfrak{o}I_\alpha$ 是一个极小左理想. 事实上, 如果 $\mathfrak{l}$ 为 $\mathfrak{o}I_\alpha$ 的一个子理想, 则由 (14.41) 可得

$$I_\alpha\mathfrak{l} \subseteq I_\alpha\Omega,$$

但 $I_\alpha\Omega$ 是一个单项的, 因而也是极小的 Ω 模, 故必有

$$I_\alpha\mathfrak{l} = I_\alpha\Omega \text{ 或 } I_\alpha\mathfrak{l} = (0).$$

在第一种情形下, 有 $\mathfrak{o}I_\alpha = \mathfrak{o}I_\alpha\Omega = \mathfrak{o}I_\alpha\mathfrak{l} \subseteq \mathfrak{l}$. 从而 $\mathfrak{l} = \mathfrak{o}I_\alpha$. 在第二种情形下, 有 $I^2 \subseteq \mathfrak{o}I_\alpha\mathfrak{l} = \{0\}$, 但 $\mathfrak{o}$ 中除 (0) 之外没有幂零理想, 故必有 $\mathfrak{l} = (0)$.

当 $\alpha > \beta$ 时, 极小左理想 $\mathfrak{o}I_\alpha$ 和 $\mathfrak{o}I_\beta$ 不可能算子同构. 事实上, 当 $\alpha > \beta$ 时, 由 (14.37) 可得

$$S_\alpha\mathfrak{o}I_\beta = S_\alpha\mathfrak{o}S_\beta A_\beta \subseteq S_\alpha\mathfrak{o}A_\beta = (0).$$

因此, 对任意 $a' \in \mathfrak{o}I_\beta$, 有

$$S_\alpha a' = 0.$$

如果 $\mathfrak{o}I_\alpha \cong \mathfrak{o}I_\beta$, 那么对任意 $a \in \mathfrak{o}I_\alpha$, 也应有

$$S_\alpha a = 0.$$

可是这一事实对 $a = I_\alpha = S_\alpha A_\alpha$ 就不成立, 因为有 $S_\alpha^2 A_\alpha = f_\alpha S_\alpha A_\alpha \neq 0$.

每个左理想 $\mathfrak{o}I_\alpha$ 给出一个不可约表示 $\mathfrak{D}_\alpha$, 并且根据以上所证, 由不同 α 所得到的表示 $\mathfrak{D}_\alpha$ 互不等价.

这样找出的 $\mathfrak{D}_\alpha$ 的个数等于 (14.33) 的解的个数. 另一方面, 这种解的个数同时也是共轭置换类的个数, 因为每个共轭置换类都是由一切能表成具有一定长度 $\alpha_1, \cdots, \alpha_h$ 的轮换之积的置换组成的, 而这些长度可按 (14.33) 中的方式排成顺序. 可是我们知道, 全部互相不等价的表示的个数等于共轭置换类的个数. 因此, *表示 $\mathfrak{D}_\alpha$ 在等价的意义之下穷尽了群 $\mathfrak{S}_n$ 的一切不可约表示.*

在上面的一切论证中, 左理想 $\mathfrak{o}I_\alpha$ 是由一种有理的方式决定的, 由此即得出*不可约表示 (及其特征标) 的有理性.*

14.8　线性变换半群

我们从一个基域 P 出发, 并考虑一组线性变换, 其方阵系数或者属于 P 本身, 或者属于 P 的一个扩域 Λ. 这样一组线性变换称为一个*半群*, 如果它在包含任意某两个变换的同时也包含着二者的乘积. 一组线性变换的*线性包*由这组线性变换的一切可能的线性组合组成, 此种线性组合的系数取自 P. 在下面我们只考虑那样的线性变换组, 它只包含有限多个在 P 上线性无关的变换, 因而它的线性包在 P 上的秩是有限的. 在这一假设之下, 一个半群的线性包就是 P 上的一个有限秩代数 $\mathfrak{A}$. 这个代数中的每个元素都是一个线性变换. 这就是说, 我们在一个忠实表示 $\mathfrak{D}$ 的形式之下给出了一个代数 $\mathfrak{A}$.

我们感到兴趣的主要问题是：当我们作域 Λ 的扩张时, 一个不可约的表示 $\mathfrak{D}$ 将按怎样的方式进行分解？

我们永远假定, 表示 $\mathfrak{D}$ 不包含零表示作为组成的部分.

下面的两个定理对整个理论具有基本的意义：

定理 1 如果表示 $\mathfrak{D}$ 完全可约, 则代数 $\mathfrak{A}$ 是半单的.

定理 2 如果表示 $\mathfrak{D}$ 是不可约的, 或者可以分解成彼此等价的不可约组成部分, 则 $\mathfrak{A}$ 是单的.

定理 1 的证明 设 $\mathfrak{R}$ 为 $\mathfrak{A}$ 的根, 那么 $\mathfrak{R}$ 中的元素在每个不可约表示之下被映成零. 由于 $\mathfrak{D}$ 为忠实表示, 故有 $\mathfrak{R}=0$.

定理 2 的证明 代数 $\mathfrak{A}$ 必然是半单的, 即 $\mathfrak{A}$ 可表成一些单代数的直和：$\mathfrak{A}=\mathfrak{a}_1+\cdots+\mathfrak{a}_s$. 根据 14.2 节, 在 $\mathfrak{A}$ 的一个不可约表示之下, 除了一个 $\mathfrak{a}_\nu$ 之外, 所有 $\mathfrak{a}_\mu$ 都被映成零. 当我们所考虑的不是一个不可约表示, 而是把同一不可约表示重复若干次时, 这一情况亦不改变. 如果表示是忠实的, 那么就只可能有一个 $\mathfrak{a}_1$, 亦即 $\mathfrak{A}$ 为单代数.

由定理 1 立即得出 Burnside 的一个定理以及 Frobenius 和 Schur 对这个定理所作的推广：

Burnside 定理 在一个绝对不可约的 n 阶方阵半群中恰有 n^2 个线性无关的方阵.

推广 如果一个方阵半群在域 Λ 中分解成绝对不可约的组成部分, 其中恰有 s 个互不等价的组成部分, 而它们的级数分别为 $n_1,\cdots,n_s$, 那么这个半群恰包含

$$n_1^2+n_2^2+\cdots+n_s^2$$

个在 Λ 上线性无关的方阵.

推广定理的证明 在域 Λ 上作出的这个半群的线性包乃是 Λ 上阶为 n_1, $n_2,\cdots,n_s$ 的 s 个全阵环的直和. 因此它在 Λ 上的秩等于 $n_1^2+n_2^2+\cdots+n_s^2$.

其次, 在一个特征为零的域上, 还有下面的迹定理成立：

迹定理 如果两个完全可约半群的方阵之间存在一个保持乘法的 1-1 对应 (或者更广一点, 如果这两个半群可以看成同一抽象半群的两个表示), 并且相应的方阵有相同的迹, 那么这两个半群 (这两个表示) 等价.

证 将两个半群中相互对应的方阵 A 和 B 相并列：

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \tag{14.42}$$

即得出一个新的完全可约半群 $\mathfrak{g}$. 这个半群的线性包是一个代数 $\mathfrak{A}$. 代数 $\mathfrak{A}$ 中的元素乃是方阵 (14.42) 的线性组合, 因而可按同一方式分解成两个部分, 其中每一部

分给出 $\mathfrak{A}$ 的一个表示. 这两个表示的迹乃是原有的方阵 A 和 B 的迹的线性组合, 因而是彼此一致的. 由此 (14.4 节) 即可断定, $\mathfrak{A}$ 的这两个表示是等价的. 这就证明了我们的断言.

如果 $\Lambda = P$, 那么根据 14.2 节立即可知定理 1 和定理 2 的逆也成立. 如果 Λ 为 P 的一个真扩域, 那么

定理 1a 如果 $\mathfrak{A}$ 是半单的而 Λ 在 P 上可分, 那么 $\mathfrak{A}$ 在 Λ 中的每个表示 $\mathfrak{D}$ 是完全可约的.

定理 2a 如果 $\mathfrak{A}$ 是 P 上的中心单代数, 那么 $\mathfrak{A}$ 在 Λ 中的每个表示 $\mathfrak{D}$ 分解成一些相互等价的组成部分.

证 根据 14.1 节, $\mathfrak{A}$ 在 Λ 中的每个表示可由 $\mathfrak{A} \times \Lambda$ 的一个表示给出. 如果 $\mathfrak{A}$ 是半单的, 而 Λ 在 P 上可分, 那么根据 13.12 节, $\mathfrak{A} \times \Lambda$ 也是半单的, 因而 $\mathfrak{A} \times \Lambda$ 在 Λ 中的每个表示是完全可约的. 如果 $\mathfrak{A}$ 是 P 上的中心单代数, 那么再一次根据 13.12 节可知, $\mathfrak{A} \times \Lambda$ 也是单代数, 因而 $\mathfrak{A} \times \Lambda$ 在 Λ 中的每个表示可分解成彼此等价的不可约组成部分. 这样就证明了上面的两个断言.

如果一个半群的线性包是 P 上的中心代数, 即线性包的中心等于基域 P, 我们就说这个半群是 P 上的中心半群.

注意到前面已经证明的定理 1 和定理 2., 可将定理 1a 和定理 2a 改述如下:

定理 1b 域 P 中的一个完全可约线性变换半群在基域 P 的每个可分扩张之下仍是完全可约的.

定理 2b 域 P 中一个中心线性变换半群在基域 P 的任意扩张之下仍是不可约的, 或者分解成彼此等价的不可约组成部分.

完全像定理 1b 一样可以证明:

定理 1c 如果 P 中一个完全可约线性半群的线性包的中心可表成若干个在 P 上可分的域的直和, 那么这个半群在基域 P 的任意扩张之下是完全可约的.

14.9 双模与代数之积

在 14.1 节中我们已经注意到, 超复系 $\mathfrak{S}$ 在一个包含着基域 P 的域 K 中的每个表示, 可由超复系 $\mathfrak{S}_K$ 的一个表示给出. 用表示模的语言叙述出来, 这就是说, 每个以 $\mathfrak{S}$ 为左算子区, K 为右算子区的模也可以看成一个 $\mathfrak{S}_K$ 左模. 证明是这样给出的, 即当我们命 $\mathfrak{S} = a_1P + \cdots + a_nP$, 从而 $\mathfrak{S}_K = a_1K + \cdots + a_nK$ 时, 用 $\mathfrak{S}_K$ 中一个元素去左乘模中元素 u 的运算由公式

$$(a_1\kappa_1 + \cdots + a_n\kappa_n)u = a_1u\kappa_1 + \cdots + a_nu\kappa_n$$

定义. 要验证 $\mathfrak{S}_K$ 模的运算规则成立是很容易的, 只是在证明结合律

$$(bc)u = b(cu)$$

时, 必须利用 K 的可交换性：如果 $b = a_1\kappa_1, c = a_2\kappa_2$(只要考虑这两个特例就够了), 则结合律可由下列关系式中得出

$$(a_1\kappa_1 \cdot a_2\kappa_2)u = (a_1a_2\kappa_1\kappa_2)u = (a_1a_2)u(\kappa_1\kappa_2),$$
$$a_1\kappa_1(a_2\kappa_2 \cdot u) = a_1\kappa_1(a_2u\kappa_2) = a_1(a_2u\kappa_2)k_1 = (a_1a_2)u(\kappa_2\kappa_1),$$

由于 $\kappa_1\kappa_2 = \kappa_2\kappa_1$, 故最后所得的两个表达式是相等的.

当 K 为一体, 或者更广一点, 当 K 为任意环时, 也可以得出类似的情况. 其办法是先构造出 K 的*逆环*, 即与 K 反同构的一个环 K'. 如果 K 是 p 上的一个代数, 那么 K' 也是 P 上的代数; 如果 K 为一体, 那么 K' 也是一体.

我们有下面的结论：

每个以 $\mathfrak{S}$ 为左算子区、K 为右算子区的模可以看成一个 $(\mathfrak{S} \times K')$ 左模.

证明和前面一样. 设 $\mathfrak{S} = a_1P + \cdots + a_nP$, 从而 $\mathfrak{S} \times K' = a_1K' + \cdots + a_nK'$. 定义

$$(a_1\kappa_1' + \cdots + a_n\kappa_n')u = a_1u\kappa_1 + \cdots + a_nu\kappa_n. \tag{14.43}$$

模的一切运算规则都很容易验证. 结合律 $(bc)u = b(cu)$ 可以证明如下：

$$(a_1\kappa_1' \cdot a_2\kappa_2')u = (a_1a_2\kappa_1'\kappa_2')u = (a_1a_2)u(\kappa_2\kappa_1),$$

$$(a_1\kappa_1')(a_2\kappa_2' \cdot u) = a_1\kappa_1'(a_2u\kappa_2) = a_1(a_2u\kappa_2)\kappa_1 = (a_1a_2)u(\kappa_2\kappa_1).$$

用同样的办法, 也可以反过来通过定义 $u\kappa = \kappa'u$ 把每个 $(\mathfrak{S} \times K')$ 左模看成一个 $\mathfrak{S}$ 左、K 右模. *并且彼此同构的 $(\mathfrak{S} \times K')$ 左模给出同构的双模, 反之亦然.*

这个事实有着多方面的应用. 从现在起我们总是假定 K 为 P 上的一个可除代数, $\mathfrak{S}$ 为 P 上一个具有单位元的单代数, 并设两个代数 $\mathfrak{S}$ 和 K 中至少有一个是 P 上的中心代数. 这时由 13.12 节可知, 积 $\mathfrak{S} \times K'$ 是单代数. 根据 14.2 节, 所有单 $(\mathfrak{S} \times K')$ 左模彼此同构, 并且全都同构于 $\mathfrak{S} \times K'$ 中的极小左理想. 因此, 所有 ($\mathfrak{S}$ 左, K 右) 双模彼此同构. 由此即知：

$\mathfrak{S}$ 在 K 中的一切不可约表示彼此等价.

由于 $\mathfrak{S}$ 是单代数, 故所有这些表示都是忠实的. 每个这样的表示都把 $\mathfrak{S}$ 同构地映成全阵环 K_r 中的一个子环 Σ. 每两个这样的表示 $s \to S_1$ 和 $s \to S_2$(它们把 $\mathfrak{S}$ 分别映成 Σ_1 和 Σ_2) 是等价的, 因此, 根据 12.4 节, 可找到一个不依赖于 s 的方阵 Q, 它把 S_1 变成 S_2：

$$S_2 = Q^{-1}S_1Q. \tag{14.44}$$

由此很容易得出：

自同构定理　设 Σ_1 和 Σ_2 是中心单代数 K_r 中的两个彼此同构的单子代数，那么 Σ_1 和 Σ_2 之间的任何一个同构对应，如果它使得基域中的每个元素不动的话，都可由 K_r 的一个内自同构，即形如 (14.44) 自同构诱导出来.

事实上，每两个这样的子代数 Σ_1 和 Σ_2 永远可以看成同一代数 $\mathfrak{S}$ 的两个表示. 如果这两个表示可约的，那么由于它们的级数同为 r，它们必分解成同样多个不可约组成的部分. 由于这些不可约组成部分彼此等价，故原来的两个表示等价.

作为一个特例，我们有下面的结论：

K_r 的每个自同构，如果它使中心 P 的元素不动的话，都是一个内自同构.

在下文中，每当我们讲到具有单位元的代数的同构或自同构的时候，所指的永远是那样的同构或自同构，它们使基域 P 中的元素不动. 一切内自同构永远是属于这一类的.

现在仍假定 $\mathfrak{S}$ 为 P 上的一个单代数，K 为 P 上的可除代数，并设两个代数 $\mathfrak{S}$ 和 K 中有一个是 P 上的中心代数. 这时 $\mathfrak{S}\times K'$ 是单代数，因而同构于某一体 Δ 上的全阵环 Δ_t. 现在让我们来看一看，关于这个体 Δ 我们能说些什么？

一般地说，Δ 乃是一个单 $(\mathfrak{S}\times K')$ 模的右自同态环，而根据本节开头处所述，这个单模可以看成一个 ($\mathfrak{S}$ 左、K 右) 双模 $\mathfrak{M}$. $(\mathfrak{S}\times K')$ 模的每个自同构给出双模 $\mathfrak{M}$ 的一个唯一的自同构，因此 Δ 同构于双模 $\mathfrak{M}$ 的右自同态环，而逆体 Δ' 则同构于双模 $\mathfrak{M}$ 的左自同态环. 我们可以直接把 Δ' 和这个左自同态环等同起来.

如果把双模 $\mathfrak{M}$ 看成 K 上的向量空间，则 $\mathfrak{S}$ 中的元素 a 诱导出这个向量空间的线性变换：

$$au = Au.$$

我们已经看到，通过表示 $a\to A$ 可将 $\mathfrak{S}$ 同构地映成 K_r 的一个子环 Σ. 根据 13.9 节，$\mathfrak{M}$ 的左自同态，亦即 Δ' 中元素，乃是这个向量空间中的那样一些线性变换 L，它们和线性变换 A 可交换：

$$LA = AL,\quad 对一切\ \ A\in\Sigma.$$

因此，环 Δ' 是 Σ在 K_r 中的中心化子，即 K_r 中的那样一些方阵所组成的环，它们和 Σ 中一切方阵 A 可交换.

这样，我们就得出了：

积的结构定理　设 $\mathfrak{S}$ 为域 P 上一个 (具有单位元的) 单代数，K 为 P 上的一个可除代数，并设这两个代数中有一个是 P 上的中心代数. 命 K' 为 K 的逆代数. 那么 $\mathfrak{S}\times K'$ 同构于一体 Δ 上的全阵环 Δ_t，$\mathfrak{S}$ 在 K 中的唯一不可约表示将 $\mathfrak{S}$ 忠实地映成 K_r 中的一个子环 Σ，Σ 在 K_r 中的中心化子反同构于 Δ.

表示 $\mathfrak{S} \to \Sigma$ 的级数即双模 $\mathfrak{M}$ 在 K 上的秩. 如将 $\mathfrak{M}$ 看成一 $(\mathfrak{S} \times K')$ 模, 那么这个模在 K' 上的秩也是 r. 可是我们可以取 $\mathfrak{M}$ 为 $\mathfrak{S} \times K'$ 的一个极小左理想 $\mathfrak{l}$, 因此这个左理想的秩是

$$(\mathfrak{l} : K') = r.$$

单环 $\mathfrak{S} \times K' \cong \Delta_t$ 乃是 t 个这样的左理想的直和, 因此它在 K' 上的秩等于 tr. 由此即得出下面的重要关系式:

$$(\Sigma : P) = (\mathfrak{S} : P) = (\mathfrak{S} \times K' : K') = tr. \tag{14.45}$$

如果我们不从 $\mathfrak{S}$ 出发, 而从 Σ 出发, 不考虑 $\mathfrak{S} \times K'$ 而考虑与之同构的代数 $\Sigma \times K'$, 那么结构定理的表述还可稍加简化. 我们在全阵环 K_r 中取一子环 Σ, 并假设 Σ 中的方阵构成一个不可约组. 其次, 设 K 或 Σ 是 P 上的中心代数. 这时结构定理断言:

定理　*$\Sigma \times K'$ 同构于一体 Δ 上的全阵环. Σ 在 K_r 中的中心化子反同构于 Δ. Σ 在 P 上的秩等于 tr.*

Σ 为一不可约线性变换组这一假定也是可以去掉的. 由于 $\Sigma \times K'$ 的单性, Σ 在 K 中的每个方阵表示是完全可约的, 并且各个不可约组成部分彼此等价. 因此, Σ 中的方阵在基的适当选择之下可写成

$$A = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_1 \end{pmatrix} \tag{14.46}$$

的形式, 其中沿着主对角线并列着 s 个小块 A_1. 方阵 A_1 形成一个不可约组 Σ_1, 我们可把上述结构定理应用于 Σ_1, Σ_1 的中心化子由所有与 Σ_1 中一切方阵 A_1 可交换的方阵 L_1 组成, 它们仍构成一个反同构于可除代数 Δ 的可除代数 Δ'. Σ 的中心化子 T 由所有方阵

$$L = \begin{pmatrix} L_{11} & \cdots & L_{1s} \\ \vdots & & \vdots \\ L_{s1} & \cdots & L_{ss} \end{pmatrix} \tag{14.47}$$

组成, 其中 L_{ik} 取自 Δ'. 因此 $T \cong \Delta'_s$.

不难看出, 按元素可交换的两个环 Σ 和 T 的秩之间存在着关系

$$(\Sigma : P)(T : P) = (K_r : P), \tag{14.48}$$

由 (14.48) 容易推出, T 的中心化子等于 Σ.

这里所建立起来的 Σ 及其中心化子 T 之间的对称关系属于“Galois 理论”的范围. 这一理论在 Jacobson 的 *Structure of Rings* 一书中第 VI 和第 VII 章中有一个更一般的处理.

现在让我们转到结构定理的应用上来.

(1) $K \times K'$的结构. 设 K 为 P 上的一个中心可除代数. 这时我们可取 $\Sigma = K$, 并应用结构定理. 在这一情况下, 方阵的阶 r 等于 $1, \Sigma$ 显然是一个不可约方阵组. K 在 K 中的中心化子 Δ' 即 K 的中心 P. 因此也有 $\Delta = P$. 秩关系式 (14.45) 给出

$$(K : P) = t.$$

这样我们就得到结果：

$K \times K'$ 是基域 P 上的全阵环. 方阵的阶 t 等于线性秩 $(K : P)$.

(2) 可除代数中的极大交换子体. 设 K 是 P 上的一个可除代数. 如果 K 本来不是 P 上的中心代数, 我们就命它的中心 Z 为新的基域 P. 现设 Σ 为 K 的极大交换子体. Σ 在 K 中的中心化子即 Σ 自身. 事实上, 如果 θ 和 Σ 中一切元素可交换, 则体 $\Sigma(\theta)$ 将是一个域, 但 Σ 是包含在 K 内的极大的域, 故 θ 必属于 Σ.

这样一来, 我们就有 $\Delta = \Sigma$, 因而 $\Sigma \times K'$ 是 Σ 上的一个全阵环. 因此, 反同构于 $\Sigma \times K'$ 的环

$$K \times \Sigma' = K \times \Sigma = K_\Sigma$$

也就是 Σ 上的全阵环, 亦即 Σ 为 K 的分裂域. 将 K_Σ 表成全阵环 Σ_t 的表示是绝对不可约的. 在 13.12 节中, 我们曾经把一个可除代数 K 在 P 的一个适当的扩域 Σ 中的绝对不可约方阵表示的级数 t 称为可除代数 K 的指数 m. 因此 $t = m$, 而 $r = 1$. 秩关系式 (14.45) 现在给出

$$(\Sigma : P) = t = m,$$

因此我们得到下面的定理：

以 P 为中心的可除代数 K 中的极大交换子体 Σ 是 K 的分裂域, 它的次数 $(\Sigma : P)$ 等于可除代数 K 的指数 m.

(3) 作为这个定理的一个应用, 让我们决定实数域 $\mathbb{R}$ 上的一切可除代数.

P 上的交换可除代数只有 P 和 $P(\mathrm{i})$, 即实数域和复数域. 现在我们假定, 可除代数 K 是非交换的. 设 Z 为 K 的中心, 而 Σ 为 K 的一个极大交换子体, 则

$$P \subseteq Z \subseteq \Sigma \subset K, \quad (\Sigma : Z) = m, \quad (K : Z) = m^2.$$

由于 K 是非交换的, 故必有 $m > 1$. Z 和 Σ 只可能是 P 或 $P(i)$. 由于 $m > 1$, 故 $\Sigma \neq Z$. 因此必有

$$\Sigma = P(i), \quad Z = P, \quad m = 2.$$

因此所要讨论的可除代数 K 之秩应是 $m^2=4$.

根据自同构定理, $P(i)$ 的那个将 i 映成 $-i$ 的自同构可由 K 的一个内自同构诱导出来, 即可找到一个元素 k, 使

$$kik^{-1}=-i. \tag{14.49}$$

由于 k 不属于 $P(i)$, 故必有 $\Sigma(k)=K$. 因此有 $K=P(i,k)$, 由 (14.49) 得

$$k^2ik^{-2}=i.$$

因此 k^2 与 i 可交换. 可是 k^2 也与 k 可交换. 故 k^2 属于 K 的中心, $k^2=a\in P$.

假如 $a\geqslant 0$, 则 $a=b^2$, 从而

$$k^2-b^2=(k-b)(k+b)=0,$$

$$k-b=0 \quad 或 \quad k+b=0,$$

因而 $k\in P$. 这是不可能的. 因此必有 $a<0$, 即 $a=-b^2(b\neq 0)$. 将 k 乘以实因子 b^{-1} 之后可以使得 $k^2=-1$, 而不致改变以上所涉及的 k 的其他性质. 这样一来, i 和 k 就满足关系：

$$ki=-ik,$$

$$i^2=k^2=-1.$$

可是这两个关系恰好刻画了四元数体. 因此, *四元数体乃是实数域上唯一的非交换可除代数*.

同样可证：有理数域 $\mathbb{Q}$ 上每个指数为 2 的中心可除代数是一个广义四元数代数.

(4) *决定全部有限体*(即具有有限多个元素的体).

设 K 为一有限体, Z 为它的中心, m 为 K 在 Z 上的指数. K 中的每个元素都必包含在一个极大交换子体 Σ 之内, 而后者在 Z 上的次数等于 m. 可是我们知道, p^n 个元素的 Galois 域 Z 的一切 m 次扩域是彼此等价的 (事实上, 它们都是添加方程 $x^q=x, q=p^{nm}$ 的根得到的). 因此, 这些极大交换子体可由它们当中的某一个, 譬如说 Σ_0, 经过 K 中元素的变形得到

$$\Sigma=\kappa\Sigma_0\kappa^{-1}.$$

如果除去 K 中的零元素不计, 则 K 成为一群 $\mathfrak{G}$, 而 Σ_0 成为一子群 $\mathfrak{H}$, Σ 成为 $\mathfrak{H}$ 的共轭子群 $\kappa\mathfrak{H}\kappa^{-1}$, 并且这些共轭子群合并起在一起能充满整个群 $\mathfrak{G}$(因为 K 中每个元素都包含在某一 Σ 之内). 可是另一方面, 我们有下面的群论定理：

引理　*有限群 $\mathfrak{G}$ 的真子群 $\mathfrak{H}$ 和它的全部共轭子群 $s\mathfrak{H}s^{-1}$ 不可能充满整个群 $\mathfrak{G}$.*

证　设 $\mathfrak{H}$ 和 $\mathfrak{G}$ 的阶分别为 n 和 N, 并设 $\mathfrak{H}$ 的指数为 j, 则 $N = j \cdot n$. 如果 s 和 s' 属于同一陪集 $s\mathfrak{H}$, 即 $s' = sh$, 则

$$s^{-1}\mathfrak{H}s'^{-1} = sh\mathfrak{H}h^{-1}s^{-1} = s\mathfrak{H}s^{-1}.$$

由此可见, 互不相同的 $s\mathfrak{H}s^{-1}$ 的个数最多等于陪集的个数 j. 如果这些 $s\mathfrak{H}s^{-1}$(其中也有 $\mathfrak{H}$) 能充满整个 $\mathfrak{G}$, 那么它们必须互不相交, 因为不然的话, 它们不可能提供我们所需要的 $N = j \cdot n$ 个元素. 可是任意两个不同的 $s\mathfrak{H}s^{-1}$ 都共同包含着群中的单位元, 它们不可能是互不相交的. 因此我们就得出了一个矛盾.

在我们所考虑的情况之下, 由引理可知 $\mathfrak{H}$ 不可能是 $\mathfrak{G}$ 的真子群. 因此 $\mathfrak{H} = \mathfrak{G}$, 从而 $K = \Sigma_0$. 因此 K 是可交换的. 这样我们就证明了：

每个具有有限多个元素的体 K 是可交换的, 因而是一 Galois 域.

这个导源于 MacLagan-Wedderburn 的定理的另一证明, 见 Witt E. *Abh. Math. Sem. Hamburg*, 1931, Bd8: 413.

14.10　单代数的分裂域

一个单代数 $\mathfrak{A}$ 可视为一个可除代数 K 上的全阵环：

$$\mathfrak{A} = K_r.$$

根据 13.12 节, K 的分裂域同时也是 $\mathfrak{A}$ 的分裂域, 反之亦然. 因此, 在讨论单代数的分裂域的时候可以局限于可除代数 K. 其次, 我们可以取 K 的中心作为基域 P, 即 K 是 P 上的中心代数.

根据 14.9 节, K 的极大交换子体是 K 的一个分裂域. 由此可见, K 具有一个在 P 上的次数为有限的分裂域 Σ. 因此, 从现在起我们只限于考虑 P 的有限扩域 Σ.

根据 14.9 节, 每个这样的域 Σ 可以不可约地嵌入 K_r 中去. 因此我们可以一上来就把 Σ 看成 K_r 中的一个不可约方阵组. 现在假设 Σ 是 K 的分裂域, 从而 $\Sigma \times K'$ 为 Σ 上的全阵代数：

$$\Sigma \times K' = \Sigma_t, \quad \text{亦即 } \Delta = \Sigma.$$

逆环 Δ' 仍是 Σ. 因此 Σ 的中心化子等于 Σ. 这就是说, K_r 中每个与 Σ 中一切元素可交换的元素包含在 Σ 之内. 由此即知, Σ 是 K_r 中的一个极大交换子体 (甚至还是 K_r 中的极大交换子环).

反之, 假设 Σ 为方阵环 K_r 中的极大交换子体. 如果 Σ 是可约的, 那么根据 (14.46), 可将 Σ 中的方阵 A 表成子方阵 A_1 的并列形状. 这些子方阵 A_1 组成一个同构于 Σ 的方阵组 Σ_1, 并且仍是极大的. 因此, 不失普遍性, 我们可以一上来就假定 Σ 是不可约的.

Σ 的中心化子 Δ' 是一个体, 它的每个元素 θ 与 Σ 中一切元素可交换. 如果这样一个元素 θ 不包含在 Σ 之内, 则 $\Sigma(\theta)$ 是 Σ 在 K_r 中的一个真包域, 与 Σ 的极大性相违. 因此必有 $\Delta' = \Sigma$. 这样一来也有 $\Delta = \Sigma$, 亦即 Σ 为 K 的分裂域.

这样, 我们就得出了分裂域的如下一个刻画:

全阵环 K_r 的每个极大交换子体是 K 的分裂域; 反之, 每个分裂域可以表示成 (甚至还可以不可约地表示成)K_r 的一个极大交换子体.

根据 (14.45), 当 Σ 不可约地嵌在 K_r 中时, 秩关系式

$$(\Sigma : P) = tr$$

成立, 其中 t 仍是 K 在 Σ 中的绝对不可约表示的级数, 即 t 等于可除代数 K 的指数 m. 因此

$$(\Sigma : P) = mr.$$

由此即知, K的分裂域 Σ 在 P 上的次数永远是 K 的指数 m 的一个倍数. K 本身中的极大交换子体乃是在 P 上具有最小次数 m 的分裂域.

最后, 我们证明下面的定理:

定理 *P 上的每个中心可除代数 K 至少有一个可分分裂域.*

为了证明这个定理, 我们要用到一个引理.

引理 *在一个特征为 p 的域中, 每个满足条件*

$$A^{p^e} = E\zeta \quad (E = \text{单位方阵}) \tag{14.50}$$

的 p^f 阶方阵 A 的特征多项式 (参看 12.6 节) 具有形式:

$$\chi(x) = x^{p^f} - \beta.$$

因而当 $p^f > 1$ 时, A 的迹等于零.

引理的证明 我们可以把 ζ 的 p^e 次根添加到基域中去, 因而可以假定 $\zeta = \eta^{p^e}$. 如果把 A 看成一个向量空间中的线性变换, 那么对任意向量 v, 有

$$0 = (A^{p^e} - \zeta)v = (A^{p^e} - \eta^{p^e})v = (A - \eta)^{p^e} v.$$

因此, 根据方阵 A 的初等因子的定义 (12.5 节), 所有初等因子 $f_\nu(x)$ 都能整除 $(x - \eta)^{p^e}$, 因而所有初等因子都是 $x - \eta$ 的幂. 特征多项式 $\chi(x)$ 乃是初等因子的乘

积, 因而也是 $(x-\eta)$ 的幂. 但 $\chi(x)$ 为 p^f 次多项式, 故有

$$\chi(x)=(x-\eta)^{p^f}=x^{p^f}-\eta^{p^f}=x^{p^f}-\beta.$$

可分分裂域存在性的证明　设 Z 为 K 的一个极大可分子域, Δ' 为 Z 在 K 中的中心化子. 根据 14.9 节中的结构定理, $Z\times K'$ 同构于一全阵环 Δ_t, 其中 Δ 与 Δ' 反同构. $Z\times K'$ 的中心是 $Z\times P=Z$, 因为 P 是 K' 的中心. 因此 Δ_t 的中心也等于 Z. 可是全阵环 Δ_t 的中心等于 Δ 的中心, 故 Δ 的中心等于 Z, 因而 Δ' 的中心等于 Z.

现设 θ 为 Δ' 中的一个不属于 Z 的元素, 则 $Z(\theta)$ 在 Z 上是不可分的, 并且它在 Z 上的简约次数等于 1, 因为不然的话, $Z(\theta)$ 将包含着一个可分子域 $\supset Z$. 因此, θ 满足一个形为

$$\theta^{p^e}=\zeta,\quad \zeta\in Z \tag{14.51}$$

的不可约方程. 当 θ 本身属于 Z 时, 这一事实也成立 $(p^e=1)$.

设 Σ 为 Δ' 中的一个极大交换子体, 则 Σ 在 Z 上的简约次数等于 1, 因而它在 Z 上的次数为 p^f. Σ 是 Δ' 的分裂域, 即 $\Delta'\times\Sigma$ 是 Σ 上的全阵环, 并且方阵的阶数为 p^f. 根据上面所证的引理, 如果 $p^f>1$, 则在这一方阵表示之下 Δ' 中每个元素的迹为零. 事实上, 如果 θ 的表示方阵为 A, 则由 (14.51) 即得方阵方程 (14.50). $\Delta'\times\Sigma$ 中的每个方阵乃是 Δ' 中的方阵的线性组合, 其系数属于方阵环的基域 Σ. 因此, 如果 $p^f>1$, 则 $\Delta'\times\Sigma$ 中一切方阵的迹都应为零. 而这一点是与 $\Delta'\times\Sigma$ 为全阵环这一事实相违的. 因此唯一的可能是：$p^f=1, Z=\Sigma$. 这就是说, Z 本身是 K 的极大交换子体, 因而是 K 的分裂域.

14.11　Brauer 群, 因子系

我们把一个固定基域 P 上的一切中心单代数分成许多类, 凡同构于同一可除中心代数 K 上的全阵环的代数均归入同一个类 $[K]$.

如果 K 与 Λ 为两个这样的可除代数, 则 $K\times\Lambda$ 仍为 P 上的一个中心单代数 (13.12 节), 因而

$$K\times\Lambda\cong\Delta_t. \tag{14.52}$$

由 (14.52) 可得

$$\begin{aligned}K_r\times\Lambda_s&=K\times P_r\times\Lambda\times P_s\cong\Delta_t\times P_{rs}\\&=\Delta\times P_t\times P_{rs}=\Delta\times P_{trs}=\Delta_{trs}.\end{aligned}$$

因此类 $[K]$ 中的代数与类 $[\Lambda]$ 中的代数的一切积属于同一个类 $[\Delta]$. 这个类我们称为类 $[K]$ 和类 $[\Lambda]$ 的积. 其次, 由于

$$K \times \Lambda \cong \Lambda \times K,$$
$$K \times (\Lambda \times \Gamma) \cong (K \times \Lambda) \times \Gamma,$$

故类的乘法满足交换律和结合律. 这个乘法也有一个单位元, 即基域 P 的类 $[P]$. 最后, 每个类 $[K]$ 有一个逆类, 这就是反同构于 K 的可除代数 K' 所决定的类 $[K']$. 因此, *P上的中心单代数的类组成一个 Abel 群*. 这个群是由 Brauer 所首先研究的, 我们称它为 Brauer*代数类群*.

以 P 上同一域 Σ 为分裂域的代数类, 组成 Brauer 群的一个子群. 事实上, 根据 13.12 节, K 的一个分裂域同时也是整个类 $[K]$ 的分裂域以及它的逆类 $[K']$ 的分裂域: K' 反同构于 K, 因而 $K' \times \Sigma$ 反同构于 $K \times \Sigma$. 如果 K 和 Λ 同以 Σ 为分裂域, 则

$$K \times \Sigma \cong \Sigma_s, \quad \Lambda \times \Sigma \cong \Sigma_t,$$

因此

$$\begin{aligned}(K \times \Lambda) \times \Sigma &\cong K \times \Sigma_t \cong K \times \Sigma \times P_t \\ &\cong \Sigma_s \times P_t = \Sigma \times P_s \times P_t \cong \Sigma_{st}.\end{aligned}$$

这就是说, Σ 是积 $K \times \Lambda$, 因而也是整个代数类 $[K \times \Lambda]$ 的分裂域.

根据 14.10 节中最后一个定理, 每个 Brauer 代数类有一个可分裂域, 譬如说, 域 $P(\theta)$. 如果除了 θ 之外还把它的共轭元素添加到 P 上去, 那么就得到一个正规可分分裂域 Σ. 根据 14.10 节, 这个域 Σ 可以不可约地表示为类 $[K]$ 中某一单代数 $\mathfrak{A} = K_r$ 中的极大交换子体.

现在我们证明: *代数 $\mathfrak{A}$ 是域 Σ 和它的 Galois 群 $\mathfrak{G}$ 在 13.3 节的意义之下的叉积*.

首先, 由 13.3 节可知, Σ 等于它自身在 $\mathfrak{A} = K_r$ 中的中心化子, 也就是说, $\mathfrak{A}$ 中与 Σ 的每个元素可交换的元素属于 Σ.

在 13.3 节中我们曾经把 Galois 群 $\mathfrak{G}$ 中的元素记作 $S, T, \cdots$, 并用 β^S 表示 Σ 中元素 β 经自同构 S 作用所得出的元素. 乘积 ST 仍由

$$\beta^{ST} = (\beta^S)^T$$

来定义.

根据 14.9 节中的自同构定理, 自同构 S 可由 $\mathfrak{A}$ 的内自同构诱导出来. 因此, 对 $\mathfrak{G}$ 中每个元素 S, 在 $\mathfrak{A}$ 中可找到一个可逆元素 u_S, 使对任意 $\beta \in \Sigma$ 有

$$u_S^{-1} \beta u_S = \beta^S,$$

或

$$\beta u_S = u_S \beta^S. \tag{14.53}$$

由 (14.53) 可以看出, 元素 $u_{ST}^{-1} u_S u_T$ 与 Σ 中一切元素可交换, 因而它本身属于 Σ. 命

$$u_{ST}^{-1} u_S u_T = \delta_{S,T},$$

那么我们就有乘法规则：

$$u_S u_T = u_{ST} \delta_{S,T}. \tag{14.54}$$

由于 $\delta_{S,T}$ 具有逆元 $u_T^{-1} u_S^{-1} u_{ST}$, 故 $\delta_{S,T} \neq 0$.

这里的式 (14.53) 和 (14.54) 恰恰就是定义叉积时所用到的式 (13.36) 和 (13.37). 在前面我们已经证明, 由这两个式子就可推出 u_S 在 Σ 上线性无关. 取 Σ 中的元素为系数作出来的 u_S 的各种线性组合

$$a = \sum_S u_S \beta_S$$

构成 $\mathfrak{A}$ 中的一个子环 $\mathfrak{A}_1$.$\mathfrak{A}_1$ 在 Σ 上的秩为 n, 因而它在 P 上的秩为 n^2, 其中 $n = (\Sigma : P)$ 为 Σ 在 P 上的次数. 根据 14.10 节, 有

$$n = (\Sigma : P) = rm.$$

$\mathfrak{A} = K_r$ 在 P 上的秩是

$$r^2 (K : P) = r^2 m^2 = n^2.$$

由于 $\mathfrak{A}_1$ 和 $\mathfrak{A}$ 有相同的秩, 并且 $\mathfrak{A}$ 包含着 $\mathfrak{A}_1$, 故应有 $\mathfrak{A}_1 = \mathfrak{A}$. 也就是说, $\mathfrak{A}$ 是域 Σ 和它的 Galois 群的叉积.

$\mathfrak{A} = K_r$ 可表成叉积这一事实是由 Noether 首先认识到的. 因此元素 $\delta_{S,T}$ 所组成的系统 $\{\delta_{S,T}\}$ 称为代数 $\mathfrak{A}$ 或代数类 $[K]$ 的 *Noether 因子系*. 显然有下面的定理：

代数 $\mathfrak{A}$ 的结构随着域 Σ 及因子系 $\{\delta_{S,T}\}$ 的给定而唯一确定.

这个定理的反面并不成立. 当 $\mathfrak{A}$ 和 Σ 给定时, 虽然 Σ 到 $\mathfrak{A}$ 内的嵌入映射除了相差 $\mathfrak{A}$ 的一个内自同构之外是唯一确定的, 可是元素 u_S 并不由这一嵌入所唯一确定, 根据 (13.39) 它们可以换成

$$v_S = u_S \gamma_S \quad (\gamma_S \neq 0). \tag{14.55}$$

作这样一种更换的自由也就是我们所仅有的自由. 事实上, 如果元素 v_S 和元素 u_S 一样具有性质 (14.53)：

$$\beta v_S = v_S \beta^S,$$

则元素 $v_S u_S^{-1}$ 和 Σ 中一切元素 β 可交换：

$$\beta v_S u_S^{-1} = v_S \beta^S u_S^{-1} = v_S u_S^{-1} \beta.$$

因此, 如命 $v_S u_S^{-1} = \gamma_S$, 则 γ_S 为 Σ 中的元素, 并且有

$$v_S = \gamma_S u_S.$$

在 13.3 节中我们已经看到, 把 u_S 更换成 v_S 时, 因子系 $\{\delta_{S,T}\}$ 就过渡到它的一个伴随因子系 $\{\varepsilon_{S,T}\}$：

$$\varepsilon_{S,T} = \frac{\gamma_S^T \gamma_T}{\gamma_{ST}} \delta_{S,T}. \tag{14.56}$$

因此, 以固定正则可分分裂域 Σ 的 Brauer 代数类 $[K]$ 和 Σ 中满足结合性条件 (13.38) 的伴随因子系的类一一对应.

直到目前为止, 我们都是从一个正规的分裂域 Σ 出发的. 根据 Brauer, 也可对单代数 K_r 的一个非正规分裂域来定义因子系.

设 Δ 为一个有限分裂域, 但不一定是正规的. 设 $\theta = \theta_1$ 为 Δ 的一个本原元素, 即 $\Delta = P(\theta)$, 并设 $\theta_\alpha (\alpha = 1, 2, \cdots, n)$ 为 θ 在一个适当的正规扩域 Σ 中的共轭元素.

在等价的意义之下, K_r 在 Δ 中只有一个 (绝对) 不可约的方阵表示. 设 $a \to A$ 为这一方阵表示, 并设 $a \to A_\alpha$ 为将域同构 $\theta \to \theta_\alpha$ 作用于这一表示中的方阵的系数之上而得到的表示. 由于这些表示彼此等价 (因为在等价意义之下, 代数 K_r 在 Σ 中也只有一个不可约表示), 故可找到方阵 $P_{\alpha\beta}$ 将表示 A_α 变形成表示 A_β：

$$A_\alpha = P_{\alpha\beta} A_\beta P_{\alpha\beta}^{-1}.$$

方阵 $P_{\alpha\beta}$ 可以取在域 $P(\theta_\alpha, \theta_\beta)$ 之内, 因为表示 $a \to A_\alpha$ 和 $a \to A_\beta$ 在这个域中就已经是等价的. 其次, 我们还可以这样来选择 $P_{\alpha\beta}$, 使得 $P(\theta_\alpha, \theta_\beta)$ 的每一个同构, 如果它把元素对 $\theta_\alpha, \theta_\beta$ 映成一共轭对 $\theta_\gamma, \theta_\delta$ 的话, 也把 $P_{\alpha\beta}$ 映成 $P_{\gamma\delta}$. 为了这一目的, 只要在元素对的每个共轭类中选出一个对 α, β 来, 就这个元素对作出 $P_{\alpha\beta}$, 并将相应的域同构作用到 $P_{\alpha\beta}$ 上去, 以定义其余的 $P_{\gamma\delta}$.

现在我们有

$$\begin{aligned} A_\alpha &= P_{\alpha\beta} A_\beta P_{\alpha\beta}^{-1} = P_{\alpha\beta} P_{\beta\gamma} A_\gamma P_{\beta\gamma}^{-1} P_{\alpha\beta}^{-1} \\ &= P_{\alpha\beta} P_{\beta\gamma} P_{\alpha\gamma}^{-1} A_\alpha P_{\alpha\gamma} P_{\beta\gamma}^{-1} P_{\alpha\beta}^{-1}. \end{aligned}$$

这就是说, 方阵 $P_{\alpha\beta} P_{\beta\gamma} P_{\alpha\gamma}^{-1}$ 和一个绝对不可约表示中的一切方阵可交换, 因此它必是单位方阵 E 的常数倍：

$$P_{\alpha\beta} P_{\beta\gamma} P_{\alpha\gamma}^{-1} = c_{\alpha\beta\gamma} E$$

$$P_{\alpha\beta}P_{\beta\gamma}=c_{\alpha\beta\gamma}P_{\alpha\gamma}. \tag{14.57}$$

Brauer因子系$\{c_{\alpha\beta\gamma}\}$ 由 (14.57) 定义. 它具有如下一些性质：

(1) $c_{\alpha\beta\gamma}$ 属于域 $P(\theta_\alpha,\theta_\beta,\theta_\gamma)$;

(2) $c_{\alpha\beta\gamma}c_{\alpha\gamma\delta}=c_{\alpha\beta\delta}c_{\beta\gamma\delta}$;

(3) $c^S_{\alpha\beta\gamma}=c_{\alpha'\beta'\gamma'}$, 其中 S 为域 $P(\theta_\alpha,\theta_\beta,\theta_\gamma)$ 的一个同构, 它把 $\theta_\alpha,\theta_\beta,\theta_\gamma$ 映成 $\theta_{\alpha'},\theta_{\beta'},\theta_{\gamma'}$.

性质 (1) 由 $c_{\alpha\beta\gamma}$ 的定义中立即得出, 性质 (2) 由方阵 $P_{\alpha\beta}$ 的结合性推出, 性质 (3) 由 $P_{\alpha\beta}$ 在同构 S 作用之下的动态推出.

如果将 $P_{\alpha\beta}$ 换成 $k_{\alpha\beta}P_{\alpha\beta}$, 其中不等于零的域元素 $k_{\alpha\beta}$ 满足方阵 $P_{\alpha\beta}$ 所满足的共轭性条件, 则因子系 $c_{\alpha\beta\gamma}$ 过渡到一个伴随因子系

$$c'_{\alpha\beta\gamma}=\frac{k_{\alpha\beta}k_{\beta\gamma}}{k_{\alpha\gamma}}c_{\alpha\beta\gamma}. \tag{14.58}$$

另一方面, 如果我们将表示 $a\to A$ 换成一个与它等价的表示 $a\to QAQ^{-1}$, 则 P_α 被换成 $Q_\alpha P_\alpha Q_\alpha^{-1}$. 很容易验证, 在这一更换之下因子系 $c_{\alpha\beta\gamma}$ 不发生改变. 因此, 因子系 $c_{\alpha\beta\gamma}$ 在伴随的意义之下由 K_r 和 Δ 所唯一确定.

我们可以把整个理论或者完全建立在 Noether 因子系的基础之上, 或者完全建立在 Brauer 因子系的基础之上. 可是, 如果我们将两种因子系同时并用, 并证明二者的同效性, 那么许多定理的证明将会来得更简单和更容易看出其意义. 事实上, 有一些性质对 Noether 因子系比较容易证明, 另一些性质对 Brauer 因子系比较容易证明. 我们先从 Brauer 因了系的一些基本性质入手.

如果 K_r 是基域 P 上的全阵环, 即 $K_r=P_r$, 则可取所有 $P_{\alpha\beta}=E$. 这时所有 $c_{\alpha\beta\gamma}$ 等于 1, 从而可知：如果一个代数在基域 P 中就已分裂, 那么它的因子系是单位因子系 $c_{\alpha\beta\gamma}=1$.

现在我们找出积 $K_r\times\varLambda_S$ 的因子系. 设 $a\to A$ 为 K_r 在域 Δ 中的不可约表示, $b\to B$ 为 $\varLambda_S$ 在同一 Δ 中的不可约表示, 那么只要将 ab 映成 Kronecker 积 $A\times B$(14.6 节), 就可得出 $K_r\times\varLambda_S$ 的一个表示. 只要计算一下这个表示的级数, 就很容易发现它是绝对不可约的. 事实上, 设 K_r 的绝对不可约表示的级数为 n, $\varLambda_S$ 的绝对不可约表示的次数为 m, 则 (据 Burnside 定理), K_r 的秩为 n^2, $\varLambda_S$ 的秩为 m^2, 因而 $K_r\times\varLambda_S$ 的秩为 n^2m^2. 但这两个表示的积表示的级数为 nm, 故积表示的级数与 $K_r\times\varLambda_S$ 的绝对不可约表示的级数一致.

现在我们可以计算积 $K_r\times\varLambda_S$ 的因子系了. 由 $A_\alpha=P^{-1}_{\alpha\beta}A_\beta P_{\alpha\beta}$ 和 $B_\alpha=Q^{-1}_{\alpha\beta}B_\beta Q_{\alpha\beta}$ 可得

$$A_\alpha\times B_\beta=(P_{\alpha\beta}\times Q_{\alpha\beta})^{-1}(A_\beta\times B_\beta)(P_{\alpha\beta}\times Q_{\alpha\beta}),$$

因此 $P_{\alpha\beta} \times Q_{\alpha\beta}$ 即积表示之间的变换方阵. 同样, 由

$$P_{\alpha\beta}P_{\beta\gamma} = c_{\alpha\beta\gamma}P_{\alpha\gamma} \quad \text{和} \quad Q_{\alpha\beta}Q_{\beta\gamma} = d_{\alpha\beta\gamma}Q_{\alpha\gamma}$$

可得

$$(P_{\alpha\beta} \times Q_{\alpha\beta})(P_{\beta\gamma} \times Q_{\beta\gamma}) = c_{\alpha\beta\gamma}d_{\alpha\beta\gamma}(P_{\alpha\gamma} \times Q_{\alpha\gamma}).$$

由此可见, $\{c_{\alpha\beta\gamma}d_{\alpha\beta\gamma}\}$是积代数 $K_r \times \Lambda_S$ 的一个因子系.

如果把这一结果应用于 $K \times P_r = K_r$ 的情形, 那么, 由于在这一情形下 $d_{\alpha\beta\gamma} = 1$, 我们就看到, 全阵环 K_r 和可除代数 K 有同一因子系. 因此, 如果把相互伴随的因子系看成相同的话, 每个 Brauer 代数类对应着同一个因子系.

总结可得下面的定理: 对 Brauer 代数类群中以 Δ 为分裂域的每个元素, 在伴随的意义下有一个唯一确定的因子系 $\{c_{\alpha\beta\gamma}\}$ 与之相应, 并且和 Brauer 群中的单位元相对应的因子系为单位因子系, 和两个群元素之积相对应的为相应的因子系之积.

现在来看一看, 当一个代数的分裂域作扩张时, 它的因子系将按怎样的方式变化. 现在设 $\Delta' = P(\theta')$ 为 $\Delta = P(\theta)$ 的一个有限可分扩张. 域 Δ' 的每个同构 $\theta' \to \theta'_{\alpha'}$ 诱导出域 Δ 的一个同构 $\theta \to \theta_\alpha$. 因此, 每个足数 a' 有一个足数 α 与之相对应. 当从 Δ 过渡到 Δ' 时, K_r 在 Δ 中的原有表示 $a \to A$ 仍可保持不变, 因而与这一表示共轭的表示 A_α 也将保持不变. 这就是说, 如果与足数 α' 相对应的足数为 α, 则有 $A'_{\alpha'} = A_\alpha$. 与此相应. 如果与足数对 α', β' 相对应的足数对为 α, β, 则对变换方阵 $P_{\alpha\beta}$ 来说也有相对应的规则 $P'_{\alpha'\beta'} = P_{\alpha\beta}$. 最后, 对因子系来说, 我们得到同样一个简单的规则: 如果与足数 α', β', γ' 相对应的足数为 α, β, γ, 也就是说, 如果域 Δ' 的同构 $\theta' \to \theta'_{\alpha'}, \theta' \to \theta'_\beta, \theta' \to \theta'_{\gamma'}$ 诱导出域 Δ 的同构 $\theta \to \theta_\alpha, \theta \to \theta_\beta$, $\theta \to \theta_\beta$, 则 $c'_{\alpha'\beta'\gamma'} = c_{\alpha\beta\gamma}$.

在这一规则的基础之上, 我们永远可以由一个任意的可分分裂域 Δ 过渡到一个包含着 Δ 的正规分裂域 Σ 去. 这时 Σ 的同构 $\theta \to \theta_\alpha$ 就是 Galois 群中的元素 $S, T, \cdots, \theta_\alpha = \theta^S, \theta_\beta = \theta^T$ 等等. 因此, 在这情形下我们可以用元素 S, T, R 等代替 α, β, γ 来作为足标, 并将 $c_{\alpha\beta\gamma}$ 改写成 $c_{S,T,R}$. 在这一新的记法之下, 性质 (3) 表现为

$$c^Q_{S,T,R} = c_{SQ,TQ,RQ}. \tag{14.59}$$

现在我们可以给出 Brauer 因子系与 Noether 因子系之间的关系了. 为此我们计算本节开头处所定义的叉积 K_r 的 Brauer 因子系, 并证明它除了记法上有所不同之外, 是和 Noether 因子系相一致的.

如果把 K_r 本身看成 Σ 上的一个表示模, 我们就得出 K_r 在 Σ 上的一个不可约表示. 当我们把 K_r 看成一个 Σ 右模时, 元素 u_S 就恰好构成它的一个基. 用元

素 $a=u_S\beta$ 去左乘一切基元素 u_T, 并将乘积按 u_T 展开：

$$(u_S\beta)u_T=u_Su_T\beta^T=u_{ST}\delta_{S,T}\beta^T,$$

就得到元素 a 的表示方阵 (只要考虑这种形状的元素就够了, 因为一切其他元素都是这种元素的和). 因此可见, 在 a 的表示方阵 A 中, 第 T 列第 ST 行的系数为 $\delta_{S,T}\beta^T$, 而该列中所有其余系数均为零. 由此即知, 共轭方阵 A^R 中第 T 列第 ST 行的系数为

$$(\delta_{S,T}\beta^T)^R=\delta_{S,T}^R\beta^{TR}.$$

现在我们要找出将表示 A 变形为表示 A^R 的方阵 $P_{1,R}$：

$$AP_{1,R}=P_{1,R}A^R. \tag{14.60}$$

我们取 $P_{1,R}$ 为那样一个方阵, 它的第 Y 列第 YR 行的系数为 $\delta_{Y,R}$, 而该列中所有其余系数为零. 这时关系式 (14.60) 就能满足, 因为在左端那个方阵中第 T 列第 STR 行的系数为 $\delta_{S,TR}\beta^{TR}\delta_{T,R}$, 在右端那个方阵中同一位置上的系数为 $\delta_{ST,R}\delta_{S,T}^R\beta^{TR}$, 而根据式 (13.38) 这两个系数是一样的. 这样, 我们就找到了所需要的方阵 $P_{1,R}$①. 其余的 $P_{S,T}$(根据定义 $P_{\alpha\beta}$ 时所作的约定) 可由 $P_{1,R}$ 经自同构 S 的作用得出

$$P_{1,R}^S=P_{S,RS}.$$

关系式 $P_{S,T}P_{T,R}=c_{S,TR}P_{S,R}$ 只要在 $S=1$ 的情形能满足即可, 因为我们总可以通过同构 S 的作用, 把足标 1 变为 S(参看 (14.59)). 因此只要考虑

$$P_{1,R}P_{R,TR}=c_{1,R,TR}P_{1,TR}$$

或

$$P_{1,R}P_{1,T}^R=c_{1,R,TR}P_{1,TR}$$

就够了. 在左端的方阵中第 S 列第 STR 行的系数为

$$\delta_{ST,R}\delta_{S,T}^R=\delta_{S,TR}\delta_{T,R},$$

而右端方阵中相应位置的系数为 $c_{1,R,TR}\delta_{S,TR}$. 因此必须命

$$c_{1,R,TR}=\delta_{T,R}. \tag{14.61}$$

根据公式 (14.61), 只要知道了 Brauer 因子系, Noether 因子系也就可以随之定出. 可是 Noether 因子系完全决定代数 K_r 的结构, 因此

Brauer 代数类由 P 的分裂域 Δ 和因子系 $\{c_{\alpha\beta\gamma}\}$ 所唯一确定.

---

① 由于 $P_{1,R}\neq 0$, 而 A 与 A^R 为不可约表示, 故知 $P_{1,R}$ 为可逆方阵.—— 译者注

在前面讨论代数的积的因子系时, 我们已经建立了具有同一分裂域 Δ 的 Brauer 代数类所组成的群到它们的伴随因子系类所组成的群上的同态. 根据适才所证的唯一性, 这个同态是一个同构.

容易看出 (13.38) 所表示的结合性条件乃是 $c_{\alpha\beta\gamma}$ 的性质 (1)~ (3) 的推论. 因此, 每给一组具有性质 (1)~ (3) 的域元素 $c_{\alpha\beta\gamma}$ 就可以找出一个代数类, 这个代数类以由公式 (14.61) 所定义的因子系 $\delta_{S,T}$ 所决定的叉积为代表.

在公式 (14.61) 的基础上, 可将 Brauer 因子系的基本性质搬到 Noether 因子系上. 特别从这里可以推出具有固定正规分裂域的代数类所组成的群与它们的伴随 (Noether) 因子系类所组成的群的同构性. 我们特别指出:

叉积 K_r 是基域 P 上的全阵环, 当且仅当 K_r 的因子系 $\delta_{S,T}$ 与单位因子系相伴随, 即

$$\delta_{S,T} = \frac{c_S^T c_T}{c_{ST}}.$$

习题 14.5 设当基域 P 扩张成扩域 Λ 时, 可除代数 K 过渡到单代数 K_Λ. 证明: Brauer 因子系将按如下方式"精简": 先将 Δ 和 Λ 都嵌入一个共同的扩域. 然后在与 θ 共轭的一切元素 θ_α 中, 把这样的一些元素选出来, 这些元素不仅对 P 来说与 θ 共轭, 而且对新的基域 Λ 来说也与 θ 共轭. 如果 $\theta_\alpha, \theta_\beta, \theta_\gamma$ 都是被选中的元素, 则保留 $c_{\alpha\beta\gamma}$, 否则就将 $c_{\alpha\beta\gamma}$ 去掉. 用 Noether 因子系的语言来说, 这就意味着只有当 S, T 都属于 Galois 群的某一确定的子群 (哪一个子群?) 时, $\delta_{S,T}$ 才有资格被保留.

习题 14.6 利用习题 14.5 解答下面的问题: Σ 中哪些子域是具有因子系 $\delta_{S,T}$ 的代数的分裂域?

习题 14.7 两个循环代数 (δ, Σ, S) 和 (ε, Σ, S) 同构, 当且仅当 δ 和 ε 的比是域 Σ 中某一元素的范数. 特别, (δ, Σ, S) 是 P 上的全阵代数, 当且仅当 δ 是 Σ 中一个元素的范数.

第 15 章 交换环的一般理想论

15.1 Noether 环

在这一章里, 我们将研究交换环的理想的整除性, 并且将考察, 例如在整数环内成立的简单规律, 在一般环上可以推广到怎样的地步. 为了避免关系复杂起见, 我们只限于这样的环, 在其中每一个理想都有一个有限基. 正如我们将要看到的那样, 实际上在很多重要的情形, 这个条件都被满足.

我们说, 在一个环 $\mathfrak{o}$ 里, 基条件成立, 如果 $\mathfrak{o}$ 中每一个理想都有一个有限基. 设有一个交换环, 如果在它里面基条件成立, 就叫做 Noether 环.

对于每一个域来说, 基条件成立, 因为只有理想 (0) 及 (1). 这个条件对于整数环, 更一般地说, 对于每一个主理想环来说都成立. 这条件对于每一有限环当然也成立. 稍后我们将看到, 如果基条件对于一个环 $\mathfrak{o}$ 成立, 那么它对于每一同余类环 $\mathfrak{o}/\mathfrak{a}$ 也成立. 最后, 我们有下面这样一个主要是由 Hilbert 给出的定理:

定理 如果基条件对于环 $\mathfrak{o}$ 成立, 且 $\mathfrak{o}$ 有单位元, 那么基条件对于多项式环 $\mathfrak{o}[x]$ 也成立.

证 设 $\mathfrak{A}$ 是 $\mathfrak{o}[x]$ 的一个理想. $\mathfrak{A}$ 的各个多项式中 x 的最高幂的系数连同零一起作成 $\mathfrak{o}$ 的一个理想, 因为若 α 与 β 是多项式 a, b 的最高系数.

$$a = \alpha x^n + \cdots,$$

$$b = \beta x^m + \cdots,$$

例如, 假定 $n \geqslant m$, 那么

$$\begin{aligned} a - bx^{n-m} &= (\alpha x^n + \cdots) - (\beta x^n + \cdots) \\ &= (\alpha - \beta)x^n + \cdots \end{aligned}$$

仍是 $\mathfrak{A}$ 的一个多项式, 而 $\alpha - \beta$ 是它的最高系数或零. 同样, 若 α 是 a 的最高系数, 那么 $\lambda\alpha$ 是 λa 的最高系数或零.

这个由最高系数所组成的理想 $\mathfrak{a}$, 根据假设有一个基 $(\alpha_1, \cdots, \alpha_r)$. 设 α_i 是 n_i 次多项式

$$a_i = \alpha_i x^{n_i} + \cdots$$

的最高系数, 并且令 n 是有限多个数 n_i 中的最大者.

我们取这些多项式 a_i 作为所要选的 $\mathfrak{A}$ 的基里的元素. 然后再看, 为了得到一个基还需要另外取哪些多项式.

设

$$f = \alpha x^N + \cdots$$

是 $\mathfrak{A}$ 中一个次数为 $N \geqslant n$ 的多项式, 那么 α 必须属于理想 $\mathfrak{a}$:

$$\alpha = \sum \lambda_i \alpha_i.$$

现在作出多项式

$$f_1 = f - \sum(\lambda_i x^{N-n_i}) a_i.$$

在这个多项式里, x^N 的系数是

$$\alpha - \sum \lambda_i \alpha_i = 0.$$

从而 f_1 有次数 $< N$. 因此可以将多项式 f 模 $(a_1, \cdots, a_p)$ 代之以一个次数较低的多项式. 我们可以按照这个方法继续下去, 直到出现次数小于 n 的多项式时为止. 因此, 以下只需考虑具有有界次数 $(< n)$ 的多项式.

$\mathfrak{A}$ 的次数 $\leqslant n-1$ 的多项式中 x^{n-1} 的系数连同零一起, 作成一个理想 $\mathfrak{a}_{n-1}$. 设

$$(\alpha_{r+1}, \cdots, \alpha_s)$$

是这个理想的一个基. 再者, 设 α_{r+i} 是多项式

$$a_{r+i} = \alpha_{r+i} x^{n-1} + \cdots$$

的最高系数. 我们再把多项式 $a_{r+1}, \cdots, a_s$ 加进所要造的基里去. 于是每一个次数 $\leqslant n-1$ 的多项式可以模 $(a_{r+1}, \cdots, a_s)$ 而代之以一个次数 $\leqslant n-2$ 的多项式. 只要像上面那样减去一个适当选取的线性组合

$$\sum \lambda_{r+i} a_{r+i}$$

即可.

如此继续下去. 在次数 $\leqslant n-2$ 的多项式中, x^{n-2} 的系数连同零一起作成一个理想 $\mathfrak{a}_{n-2}$, 它的基元素 $\alpha_{s+1}, \cdots, \alpha_t$ 属于多项式 $a_{s+1}, \cdots, a_t$. 我们再把这些多项式加进所要造的基里去. 最后, 我们达到只由 $\mathfrak{A}$ 里的常数所组成的理想 $\mathfrak{a}_0$. 它的基 $(\alpha_{\nu+1}, \cdots, \alpha_w)$ 属于多项式 $a_{\nu+1}, \cdots, a_w$. $\mathfrak{A}$ 中每一多项式模

$$(a_1, \cdots, a_r, a_{r+1}, \cdots, a_s, \cdots, a_{\nu+1}, \cdots, a_w)$$

最后必定约简为零. 于是, 多项式 $a_1, \cdots, a_w$ 作成理想 $\mathfrak{A}$ 的一个基, 从而基条件成立.

将这个定理应用 n 次, 我们立刻得到以下的拓广:

如果对于一个具有单位元的环 $\mathfrak{o}$ 来说基条件成立, 那么这个条件对于有限个不定元 $x_1, \cdots, x_n$ 的多项式环 $\mathfrak{o}[x_1, \cdots, x_n]$ 也成立.

最重要的特例是: 整系数多项式环 $\mathbb{Z}[x_1, \cdots, x_n]$ 和系数在一个域 K 内的多项式环 $K[x_1, \cdots, x_n]$. 所有这些环都是 Noether 环.

Hilbert 只对这样的情形叙述了他的定理, 而在形式上看起来或者更一般些, 即

在 $\mathfrak{o}$ 的每一子集 $\mathfrak{M}$ 中 (不仅在每一理想中) 存在有限个元素 $m_1, \cdots, m_r$, 使得 $\mathfrak{M}$ 中每一元素 m 都可以写成

$$\lambda_1 m_1 + \cdots + \lambda_r m_r \quad (\lambda_i \text{属于} \mathfrak{o})$$

的形式.

然而, 这个定理不过是理想的基条件的直接推论. 因为如果 $\mathfrak{A}$ 是由 $\mathfrak{M}$ 所生成的理想, 那么首先 $\mathfrak{A}$ 有一个基:

$$\mathfrak{A} = (a_1, \cdots, a_s).$$

每一元素 a_i(作为 $\mathfrak{M}$ 所生成的理想的元素) 依赖于 $\mathfrak{M}$ 中有限个元素:

$$a_i = \sum_k \lambda_{ik} m_{ik}.$$

所以 $\mathfrak{A}$ 的一切元素都与这有限个 m_{ik} 线性相关. 特别对于 $\mathfrak{M}$ 的元素来说, 这一事实成立.

更重要的是, 基条件还与以下的“因子链条件”等价:

因子链条件, 第一种表述　*如果在 $\mathfrak{o}$ 中给定理想 $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \cdots$ 的一个链, 而每一 $\mathfrak{a}_{i+1}$ 都是 $\mathfrak{a}_i$ 的一个真因子:*

$$\mathfrak{a}_i \subset \mathfrak{a}_{i+1},$$

那么这个链在有限项后终止.

这个条件等价于

因子链条件, 第二种表述　*如果给定因子 $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \cdots$ 的一个无限链:*

$$\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1},$$

那么自某一 n 后, 一切项必须相等:

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots.$$

由基条件推出因子链条件, 可以这样看出：

设 $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \cdots$ 是一个有限链且 $\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$. 一切理想 $\mathfrak{a}_i$ 的并 $\mathfrak{o}$ 是一个理想. 因为如果 a 与 b 属于 $\mathfrak{o}$, 例如, 设 a 属于 $\mathfrak{a}_n$ 而 b 属于 $\mathfrak{a}_m$, 那么 a 与 b 同属于 $\mathfrak{a}_N$, 此外 N 是数 n 与 m 中较大的一个. 所以 $a-b$ 也属于 $\mathfrak{a}_N$, 从而属于 $\mathfrak{o}$. 又设 a 属于 $\mathfrak{o}$, 例如 a 属于 $\mathfrak{a}_n$, 那么 $\lambda\alpha$ 也属于 $\mathfrak{a}_n$, 从而属于 $\mathfrak{o}$.

根据假设, 这个理想 $\mathfrak{o}$ 有一个基 $(a_1, \cdots, a_r)$. 每一 a_i 属于某一理想 $\mathfrak{a}_{n_i}$. 设 n 是数 n_i 中最大的一个, 那么 $a_1, \cdots, a_r$ 同在 $\mathfrak{a}_n$ 内. $\mathfrak{o}$ 中一切元素都与 $a_1, \cdots, a_r$ 线性相关, 所以 $\mathfrak{o}$ 中一切元素都属于 $\mathfrak{a}_n$, 从而得到

$$\mathfrak{o} = \mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots .$$

反过来, 由因子链条件可以推出基条件. 设 $\mathfrak{a}$ 是一个理想, a_1 是 $\mathfrak{a}$ 中任意元素. 若 a_1 不生成整个的理想, 那么在 $\mathfrak{a}$ 中还有不属于 (a_1) 的元素, 令 a_2 是这样的一个元素. 于是有

$$(a_1) \subset (a_1, a_2).$$

若 a_1 与 a_2 还不能生成整个理想, 那么同样在 $\mathfrak{a}$ 中有第三个元素 a_3, 它不属于 (a_1, a_2), 如此等等. 于是我们得到一个因子链：

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots ,$$

它在有限步 (例如 r 步) 后必定终止. 因此

$$(a_1, a_2, \cdots, a_r) = \mathfrak{a}.$$

从而 $\mathfrak{a}$ 有一个有限基.

如果在一个环 $\mathfrak{o}$ 中, 因子链条件成立, 那么在每一同余类环 $\mathfrak{o}/\mathfrak{a}$ 中, 这个条件也成立.

证 $\mathfrak{o}/\mathfrak{a}$ 中一个理想 $\overline{\mathfrak{b}}$ 是一个同余类的集. 我们做一切这样同余类的并, 于是就得到 $\mathfrak{o}$ 中的一个理想 $\mathfrak{b}$. 反过来, $\overline{\mathfrak{b}}$ 由 $\mathfrak{b}$ 通过

$$\overline{\mathfrak{b}} = \mathfrak{b}/\mathfrak{a}$$

唯一确定. 在 $\mathfrak{o}/\mathfrak{a}$ 中的一个理想链 $\overline{\mathfrak{b}}_1 \subset \overline{\mathfrak{b}}_2 \subset \overline{\mathfrak{b}}_3 \subset \cdots$ 按这种方式产生 $\mathfrak{o}$ 中的一个理想链 $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \mathfrak{b}_3 \subset \cdots$, 而由于后者在有限项终止, 所以前者也必定如此.

这样也就证明了在本节开始时所提出的论断, 即由 $\mathfrak{o}$ 中基条件成立推出在 $\mathfrak{o}/\mathfrak{a}$ 中基条件成立.

因子链条件还可以有两种其他的表述方式, 它们在应用上往往比较方便.

因子链条件, 第三种表述: 极大条件 如果在 $\mathfrak{o}$ 中因子链条件成立, 那么在每一个由理想所组成的非空集中, 都存在一个极大理想, 就是这样的理想, 它不包含在这个集中任何其他理想之内.

证 设在理想的每一个非空集中, 指定一个理想. 现在假定在一个理想的集 $\mathfrak{M}$ 中没有极大理想. 那么这个集中的每一理想还会包含在这个集的另一理想之内, 我们在 $\mathfrak{M}$ 中找出所指定的那个理想 $\mathfrak{a}_1$, 再由 $\mathfrak{M}$ 中那些包含着 $\mathfrak{a}_1$ 且 $\neq \mathfrak{a}_1$ 的理想所成的集中找出所指定的理想 $\mathfrak{a}_2$, 等等, 于是就得到一个无限的链

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots,$$

根据假设, 这是不可能的.

因子链条件, 第四种表述: 因子归纳原理 设在 $\mathfrak{o}$ 中因子链条件成立, 并设有一个性质 E. 如果对于每一理想 $\mathfrak{a}$(特别也对于单位理想) 来说, 由 E 对 $\mathfrak{a}$ 的一切真因子成立可以推出 E 对 $\mathfrak{a}$ 成立, 那么性质 E 对于一切理想成立.

证 假定这个性质 E 对于某一个理想来说不成立. 于是根据因子链条件的第三种表述, 存在一个极大理想 $\mathfrak{a}$, 它也不具有性质 E. 由于极大性, $\mathfrak{a}$ 的一切真因子必须具有性质 E, 从而 $\mathfrak{a}$ 也具有性质 E, 这是一个矛盾.

15.2 理想的积与商

如同在 3.6 节那样, 我们把理想 $\mathfrak{a}, \mathfrak{b}, \cdots$ 的最大公因子或和理解为由它们的并所生成的理想 $(\mathfrak{a}, \mathfrak{b}, \cdots)$, 同样地, 把它们的最小公倍理解为交 $[\mathfrak{a}, \mathfrak{b}, \cdots] = \mathfrak{a} \cap \mathfrak{b} \cap \cdots$. 对于由有些是元素有些是理想所生成的理想, 我们也使用与理想和的同样记法, 例如:

$$(\mathfrak{a}, b) = (\mathfrak{a}, (b)).$$

显然有 $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{b}, \mathfrak{a}), ((\mathfrak{a}, \mathfrak{b}), \mathfrak{c}) = (\mathfrak{a}, (\mathfrak{b}, \mathfrak{c})) = (\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$ 等等. 再者,

$$((a_1, a_2, \cdots), (b_1, b_2, \cdots)) = (a_1, a_2, \cdots, b_1, b_2, \cdots),$$

这就是说, 依次写下各个理想的基, 就得到最大公因子的一个基.

把理想 $\mathfrak{a}$ 的元素乘以理想 $\mathfrak{b}$ 的元素, 那么积 ab 一般来说 (与和相反) 并不作成一个理想①. 由一切这样的积 ab 所生成的理想叫做理想 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的积, 并且记作 $\mathfrak{a} \cdot \mathfrak{b}$ 或 $\mathfrak{a}\mathfrak{b}$. 它是由一切和 $\sum a_i b_i (a_i$ 属于 $\mathfrak{a}$, b_i 属于 $\mathfrak{b})$ 所组成的.

显然有

$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a},$$

① 例如, 在一个多项式环里, 若 $\mathfrak{a} = (x, y), \mathfrak{b} = (x^2, y)$, 那么 x^3 和 y^2 都是形式如 $a \cdot b$ 的积, 然而 $x^3 - y^2$ 就不是.

$$(\mathfrak{a}\cdot\mathfrak{b})\cdot\mathfrak{c}=\mathfrak{a}\cdot(\mathfrak{b}\cdot\mathfrak{c}).$$

因此, 对于理想的积, 可以像对通常的积那样来进行运算. 特别, 当说到一个理想的幂 $\mathfrak{a}^\rho$ 时有意义, 它是由

$$\mathfrak{a}^1=\mathfrak{a},\quad \mathfrak{a}^{\rho+1}=\mathfrak{a}\cdot\mathfrak{a}^\rho$$

定义的.

若 $\mathfrak{a}=(a_1,\cdots,a_n),\mathfrak{b}=(b_1,\cdots,b_m)$, 那么积 $\mathfrak{ab}$ 显然是由积 a_ib_k 生成的. 于是, 将一个因子的全部基元素乘以另一因子的全部基元素就得到积的一个基.

特别对于主理想来说,

$$(a)\cdot(b)=(ab),$$

因此, 在 $\mathfrak{o}$ 的主理想范围内乘积的定义与通常元素的乘积定义一致.

一个任意理想与一个主理想的积 $\mathfrak{a}\cdot(b)$ 由一切积 ab 所组成, 其中 a 属于 $\mathfrak{a}$. 因此我们就简写作 $\mathfrak{a}b$ 或 $b\mathfrak{a}$.

另一运算规则就是"理想的分配律":

$$\mathfrak{a}\cdot(\mathfrak{b},\mathfrak{c})=(\mathfrak{a}\cdot\mathfrak{b},\mathfrak{a}\cdot\mathfrak{c}). \tag{15.1}$$

因为 $\mathfrak{a}\cdot(\mathfrak{b},\mathfrak{c})$ 是由积 $a(b+c)$ 所生成的, 一切这样的积, 由于

$$a(b+c)=ab+ac,$$

都属于 $(\mathfrak{a}\cdot\mathfrak{b},\mathfrak{a}\cdot\mathfrak{c})$; 反过来, $(\mathfrak{a}\cdot\mathfrak{b},\mathfrak{a}\cdot\mathfrak{c})$ 是由积 ab 与 ac 生成的, 它们都属于 $\mathfrak{a}\cdot(\mathfrak{b},\mathfrak{c})$.

如果在括弧里, 用多个甚至无限多个理想来代替 $\mathfrak{b},\mathfrak{c}$, 规则 (15.1) 也成立.

因为一切积 ab 都属于 $\mathfrak{a}$, 所以

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq\mathfrak{a},$$

同样

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq\mathfrak{b},$$

从而

$$\mathfrak{a}\cdot\mathfrak{b}\subseteq[\mathfrak{a},\mathfrak{b}],$$

这就是说, 积可以被最小公倍整除.

在整数环里, 两个理想 $\mathfrak{a},\mathfrak{b}$ 的最小公倍与最大公因子的积等于 $\mathfrak{ab}$. 这一事实在任意环里不再成立. 然而有

$$[\mathfrak{a}\cap\mathfrak{b}]\cdot(\mathfrak{a},\mathfrak{b})\subseteq\mathfrak{ab}. \tag{15.2}$$

证　$[\mathfrak{a}\cap\mathfrak{b}]\cdot(\mathfrak{a},\mathfrak{b})=([\mathfrak{a}\cap\mathfrak{b}]\cdot\mathfrak{a},\quad[\mathfrak{a}\cap\mathfrak{b}]\cdot\mathfrak{b})\subseteq(\mathfrak{b}\cdot\mathfrak{a},\mathfrak{a}\cdot\mathfrak{b})=\mathfrak{a}\cdot\mathfrak{b}.$

由所考虑的环的一切元素所组成的理想 $\mathfrak{o}$ 叫做单位理想. 自然有

$$\mathfrak{a}\cdot\mathfrak{o}\subseteq\mathfrak{a}.$$

然而, 若 $\mathfrak{o}$ 含有单位元 e, 那么反过来也对

$$\mathfrak{a}=\mathfrak{a}\cdot e\subseteq\mathfrak{a}\cdot\mathfrak{o},$$

从而

$$\mathfrak{a}\cdot\mathfrak{o}=\mathfrak{a}.$$

在这个情形, 理想 $\mathfrak{o}$ 扮演着乘法中单位元的角色. 它是由单位元生成的.

我们永远有

$$(\mathfrak{a},\mathfrak{o})=\mathfrak{o},\quad\mathfrak{a}\cap\mathfrak{o}=\mathfrak{a}.$$

设 $\mathfrak{a}$ 是一个理想. 所谓理想商 $\mathfrak{a}:\mathfrak{b}$指的是 $\mathfrak{o}$ 中满足条件

$$\gamma b\equiv 0(\mathfrak{a}),\quad \text{对一切 } b \text{ 属于}\mathfrak{b} \tag{15.3}$$

的元素 γ 的全体. 这些元素的全体是一个理想. 因为当 γ 和 δ 具有性质 (15.3) 时, $\gamma-\delta$ 也具有这个性质, 又当 γ 具有性质 (15.3) 时, $r\gamma$ 也具有这个性质. 在这里只假设 $\mathfrak{a}$ 是一个理想, $\mathfrak{b}$ 并不一定是理想, 它可以是某一个集或者是单独一个元素.

由定义推出, 当 $\mathfrak{a}$ 与 $\mathfrak{b}$ 都是理想时,

$$\mathfrak{b}\cdot(\mathfrak{a}:\mathfrak{b})\subseteq\mathfrak{a}.$$

在整数环里, 两个主理想 $(a),(b)\neq 0$ 的商是这样构成的, 即由数 a 的因子分解中去掉同时出现在 b 里的因子. 例如

$$(12):(2)=(6),$$

$$(12):(4)=(3),$$

$$(12):(8)=(3),$$

$$(12):(5)=(12).$$

换一句话说, 在通常意义下用最大公因子 (a,b) 去除 a.

在一般环里, 有一个相应的规则

$$\mathfrak{a}:\mathfrak{b}=\mathfrak{a}:(\mathfrak{a},\mathfrak{b}),$$

这一点很容易证明, 而且也不十分重要.

显然 $\mathfrak{a} \subseteq \mathfrak{a} : \mathfrak{b}$, 因为 $\mathfrak{a}$ 中每一元素都具有性质 (15.3). 因此有两个极端情形:

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{o} \quad \text{及} \quad \mathfrak{a} : \mathfrak{b} = \mathfrak{a}.$$

第一个情形当 $\mathfrak{b} \subseteq \mathfrak{a}$ 时出现, 因为这时对于每一 γ,

$$\gamma b \equiv 0(\mathfrak{b}) \equiv 0(\mathfrak{a}).$$

第二个情形意味着由 $\gamma\mathfrak{b} \equiv 0(\mathfrak{a})$ 得出 $\gamma \equiv 0(\mathfrak{a})$. 因此, 在同余式 $\gamma\mathfrak{b} \equiv 0(\mathfrak{a})$ 中可以约去 $\mathfrak{b}$. 在这一情形就说 *$\mathfrak{b}$与$\mathfrak{a}$互素*. 不过我们很少使用这个容易发生误解的说法, 而常常直接写出方程 $\mathfrak{a} : \mathfrak{b} = \mathfrak{a}$. 在整数 a 与 b 都不等于零的情形, 判定标准

$$\text{由}\gamma b \equiv 0(a) \quad \text{推出}\gamma \equiv 0(a)$$

显然仅当 a 与 b 没有公共素因子时才成立. 然而在一般情形"互素"一词不是对称的. 例如, 当 $\mathfrak{a}$ 是一个素理想而 $\mathfrak{b}$ 是 $\mathfrak{a}$ 的一个异于 $\mathfrak{o}$ 的真素因子时, 有

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{a}, \quad \text{从而 } \mathfrak{b} \text{ 与 } \mathfrak{a} \text{ 互素},$$

然而

$$\mathfrak{b} : \mathfrak{a} = \mathfrak{o}, \quad \text{从而 } \mathfrak{a} \text{ 不与 } \mathfrak{b} \text{ 互素}.$$

例如

$$(0) : (2) = (0),$$

$$(2) : (0) = (1).$$

以下的运算规则是重要的:

$$[\mathfrak{a}_1, \cdots, \mathfrak{a}_r] : \mathfrak{b} = [\mathfrak{a}_1 : \mathfrak{b}, \cdots, \mathfrak{a}_r : \mathfrak{b}]. \tag{15.4}$$

证　由

$$\gamma\mathfrak{b} \subseteq [\mathfrak{a}_1, \cdots, \mathfrak{a}_r]$$

推出, 对于每一 i,

$$\gamma\mathfrak{b} \subseteq \mathfrak{a}_i.$$

反过来也对.

习题 15.1　证明下列运算规则:

$$(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \mathfrak{a} : \mathfrak{b}\mathfrak{c} = (\mathfrak{a} : \mathfrak{c}) : \mathfrak{b},$$

$$\mathfrak{a} : (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}) \cap (\mathfrak{a} : \mathfrak{c}).$$

习题 15.2 证明下列三个论断是等价的：

(a) $\mathfrak{a} : \mathfrak{b}_1 = \mathfrak{a}$ 且 $\mathfrak{a} : \mathfrak{b}_2 = \mathfrak{a}$;

(b) $\mathfrak{a} : (\mathfrak{b}_1 \cap \mathfrak{b}_2) = \mathfrak{a}$;

(c) $\mathfrak{a} : \mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{a}$.

15.3 素理想与准素理想

我们以前已经定义过素理想是这样的理想, 它的同余类环没有零因子.

在整数环里, 每一个整数 $a > 0$ 都是不相同的素数幂的积

$$a = p_1^{\sigma_1} \cdots p_r^{\sigma_r}, \tag{15.5}$$

从而每一个理想 (a) 都是素理想幂的积：

$$(a) = (p_1)^{\sigma_1} \cdots (p_r)^{\sigma_r}.$$

在更一般的环里, 我们不能希望理想的分解规律如此简单. 例如, 在一个不定元 x 的整系数多项式环里, 理想 $(4, x)$ 不是素理想, 除 $\mathfrak{o}$ 外只有一个素因子 $(2, x)$. 然而理想 $(4, x)$ 不能表示成 $(2, x)$ 的任何幂. 因此, 一般不能希望把一个理想表示成若干理想的积, 至多只能希望把理想表示成一些尽可能简单的成分的最小公倍[①]. 这种表示相当于由 (15.5) 所得出的 (a) 被表成最小公倍的如下表示：

$$(a) = [(p_1^{\sigma_1}), \cdots, (p_r^{\sigma_r})].$$

理想 $(p_k^{\sigma_k})$ 具有以下特性：若积 ab 能被 $p_k^{\sigma_k}$ 整除而因子 a 不能被 $p_k^{\sigma_k}$ 整除, 那么另一个因子 b 至少要含有 $p_k^{\sigma_k}$ 的一个因子. 这意味着某一幂 b^ρ 必须能被 $p_k^{\sigma_k}$ 整除. 因此, 由

$$ab \equiv 0(p^\sigma),$$

$$a \not\equiv 0(p^\sigma)$$

就推出

$$b^\rho \equiv 0(p^\sigma).$$

具有这样性质的理想叫做准素理想.

---

① 一个最小公倍表示在某些情形比一个积表示更有用, 就是当我们打算判断一个元素 b 能否被一个理想 $\mathfrak{m}$ 整除时, 也就是说, b 是否属于 $\mathfrak{m}$ 时. 若 $\mathfrak{m}=[\mathfrak{a}_1, \cdots, \mathfrak{a}_r]$, 那么 b 属于 $\mathfrak{m}$ 当且仅当 b 属于所有 $\mathfrak{a}_\nu$.

一个理想 $\mathfrak{q}$ 叫做一个准素理想, 如果由

$$ab \equiv 0(\mathfrak{q}), \quad a \not\equiv 0(\mathfrak{q})$$

可以得出, 存在一个 ρ 使得

$$b^\rho \equiv 0(\mathfrak{q}).$$

这个定义也可以如下叙述:

在模 $\mathfrak{q}$ 的同余类环中, 若 $\overline{a}\,\overline{b} = 0$ 且 $\overline{a} \neq 0$, 那么某一幂 $\overline{b}^\rho$ 必须等于零.

若 $\overline{a}\overline{b} = 0$ 而 $\overline{a} \neq 0$, 那么这就意味着 $\overline{b}$ 是一个零因子. 环的一个元素 b 叫做幂零的, 如果某一幂 b^ρ 等于零. 因此也可以说:

一个理想叫做准素的, 如果在它的同余类环里每一个零因子都是幂零的.

我们可以看出, 这个定义是素理想定义的一个微小改变. 在以一个素理想为模的同余类环里, 每一个零因子不仅是幂零的, 而且本身就是零.

我们将要看到, 在一般环里, 准素理想扮演着与整数环里素数幂同样的角色. 在非常一般的假设之下, 每一个理想都可以表示成准素理想的交, 并且在这个表示里, 理想的主要构造性质完全被显示出来.

准素理想不一定是素理想的幂. 这一点可由开始时所举出的理想 $(4, x)$ 来说明, 我们很容易证明这个理想是准素的. 反过来也不一定成立. 因为在 a_1 能被 3 整除的整系数多项式 $a_0 + a_1x + \cdots + a_nx^n$ 的环里, $\mathfrak{p} = (3x, x^2, x^3)$ 是一个素理想, 然而 $\mathfrak{p}^2 = (9x^2, 3x^3, x^4, x^5, x^6)$ 不是准素的, 因为

$$\begin{aligned} 9 \cdot x^2 &\equiv 0(\mathfrak{p}^2), \\ x^2 &\not\equiv 0(\mathfrak{p}^2), \end{aligned}$$

而对每一 ρ,

$$9^\rho \not\equiv 0(\mathfrak{p}^2).$$

准素理想与因子链条件无关的性质

定理 1 相应于每一个准素理想 $\mathfrak{q}$, 都存在一个素理想因子 $\mathfrak{p}$, 它是如下定义的: $\mathfrak{p}$ 是一切这样的元素 b 的全体, b 的某一个幂 b^ρ 属于 $\mathfrak{q}$.

证 第一, $\mathfrak{p}$ 是一个理想. 因为由 $b^\rho \equiv 0(\mathfrak{q})$ 得出 $(rb)^\rho \equiv 0(\mathfrak{q})$, 并且由 $b^\rho \equiv 0(\mathfrak{q})$ 及 $c^\sigma \equiv 0(\mathfrak{q})$ 得出

$$(b - c)^{\rho+\sigma-1} \equiv 0(\mathfrak{q}),$$

这是由于在 $(b - c)^{\rho+\sigma-1}$ 的展开式中每一个被加项或者含有 b^ρ 或者含有 c^σ.

第二, $\mathfrak{p}$ 是素理想. 因为由

$$ab \equiv 0(\mathfrak{p}),$$

$$a \not\equiv 0(\mathfrak{p})$$

得出, 存在一个 ρ, 使得

$$a^\rho b^\rho \equiv 0(\mathfrak{q}),$$

且

$$a^\rho \not\equiv 0(\mathfrak{q}).$$

因此必定有一个 σ, 使得

$$b^{\rho\sigma} \equiv 0(\mathfrak{q}).$$

从而

$$b \equiv 0(\mathfrak{p}).$$

第三, $\mathfrak{p}$ 是 $\mathfrak{q}$ 的因子:

$$\mathfrak{q} \equiv 0(\mathfrak{p}).$$

因为 $\mathfrak{q}$ 的元素自然具有这个性质, 即元素的一个幂属于 $\mathfrak{q}$.

$\mathfrak{p}$ 叫做属于 $\mathfrak{q}$ 的素理想, $\mathfrak{q}$ 叫做属于 $\mathfrak{p}$ 的准素理想. 由准素理想的定义推出:

定理 2 若 $ab \equiv 0(\mathfrak{q})$ 且 $a \not\equiv 0(\mathfrak{q})$, 则 $b \equiv 0(\mathfrak{p})$.

以下的定理可以说是这个定理的逆命题:

定理 3 设 $\mathfrak{p}$ 与 $\mathfrak{q}$ 是理想, 并且具有下列性质:

(1) 若 $ab \equiv 0(\mathfrak{q})$ 且 $a \not\equiv 0(\mathfrak{q})$, 则 $b \equiv 0(\mathfrak{p})$;

(2) $\mathfrak{q} \equiv 0(\mathfrak{p})$;

(3) 若 $b \equiv 0(\mathfrak{p})$ 则 $b^\rho \equiv 0(\mathfrak{q})$.

那么 $\mathfrak{q}$ 是准素理想而 $\mathfrak{p}$ 是属于 $\mathfrak{q}$ 的素理想.

证 由 $ab \equiv 0(\mathfrak{q})$ 及 $a \not\equiv 0(\mathfrak{q})$ 推出 $b^\rho \equiv 0(\mathfrak{q})$(根据 (1), (3)). 所以 $\mathfrak{q}$ 是准素的. 我们只需证明, $\mathfrak{p}$ 恰由这样的元素 b 所组成, b 的某一幂 b^ρ 属于 $\mathfrak{q}$. 这个论断的一半正是 (3). 剩下的就是要证明, 由 $b^\rho \equiv 0(\mathfrak{q})$ 推出 $b \equiv 0(\mathfrak{p})$. 设 ρ 是使得 $b^\rho \equiv 0(\mathfrak{q})$ 成立的最小自然数. 对于 $\rho = 1$, 根据 (2), 论断是正确的. 对于 $\rho > 1$, 我们有 $b \cdot b^{\rho-1} \equiv 0(\mathfrak{q})$ 而 $b^{\rho-1} \not\equiv 0(\mathfrak{q})$, 从而 $b \equiv 0(\mathfrak{p})$(根据 (1)).

这个定理在一些特殊情形下简化了准素性质的验证和属于它的素理想的寻求, 并且指出, 属于它的素理想由怎样的性质唯一确定.

当 a 与 b 用理想 $\mathfrak{a}$ 与 $\mathfrak{b}$ 代替时, 定理 2 也成立:

定理 4 若 $\mathfrak{a}\mathfrak{b} \equiv 0(\mathfrak{q})$ 且 $\mathfrak{a} \not\equiv 0(\mathfrak{q})$, 则 $\mathfrak{b} \equiv 0(\mathfrak{p})$.

因为若 $\mathfrak{b} \not\equiv 0(\mathfrak{p})$, 那么在 $\mathfrak{b}$ 中将有一个元素 b 不属于 $\mathfrak{p}$, 同时又有 $\mathfrak{a}$ 中一个元素 a 不属于 $\mathfrak{q}$. 然后乘积 ab 必须属于 $\mathfrak{ab}$, 从而属于 $\mathfrak{q}$, 这与以前所证明的性质矛盾.

类似地, 可以证明关于素理想的相应定理：

若 $\mathfrak{ab} \equiv 0(\mathfrak{p})$ 且 $\mathfrak{a} \not\equiv 0(\mathfrak{p})$, 则 $\mathfrak{b} \equiv 0(\mathfrak{p})$.

作为一个推论 (应用 $(h-1)$ 次来证明), 我们有

若 $\mathfrak{a}^h \equiv 0(\mathfrak{p})$, 则 $\mathfrak{a} \equiv 0(\mathfrak{p})$.

定理 4 的另一种表述是

定理 4′ 若 $\mathfrak{b} \not\equiv 0(\mathfrak{p})$, 则 $\mathfrak{q} : \mathfrak{b} = \mathfrak{q}$.

同余类环 $\mathfrak{o}/\mathfrak{q}$ 包含理想 $\mathfrak{p}/\mathfrak{q}$(因为 $\mathfrak{p} \supseteq \mathfrak{q}$). 这个理想是由一切幂零元素组成的, 从而当 $\mathfrak{q} \neq \mathfrak{o}$ 时由一切零因子所组成.

准素理想在有因子链条件的假定下的性质

设 $\mathfrak{p}$ 是属于 $\mathfrak{q}$ 的素理想, 那么 $\mathfrak{p}$ 中每一元素的某一幂属于 $\mathfrak{q}$. 对于这个幂所必须的最小指数依赖于元素的选取, 并且可以无限增大. 然而, 如果在环 $\mathfrak{o}$ 中假定因子链条件成立, 那么这样的指数不能无限增大, 因为有以下的定理：

定理 5 一个幂 $\mathfrak{p}^\rho$ 可以被 $\mathfrak{q}$ 整除：

$$\mathfrak{p}^\rho \equiv 0(\mathfrak{q}).$$

证 设 $(p_1, \cdots, p_r)$ 是 $\mathfrak{p}$ 的一个基. 又设 $p_1^{\rho_1}, \cdots, p_r^{\rho_r}$ 属于 $\mathfrak{q}$. 如果令

$$\rho = \sum_1^r (\rho_i - 1) + 1,$$

那么 $\mathfrak{p}^\rho$ 由一切 p_i 的每次取 ρ 个因子的积所生成. 在每一个这样的积里, 至少有一个因子 p_i 必须出现多于 $(\rho_i - 1)$ 次, 从而至少出现 ρ_i 次. 所以 $\mathfrak{p}^\rho$ 的一切生成元都属于 $\mathfrak{q}$, 定理被证明.

在一个准素理想 $\mathfrak{q}$ 与属于它的素理想 $\mathfrak{p}$ 之间以下关系成立：

$$\mathfrak{q} \equiv 0(\mathfrak{p}),$$

$$\mathfrak{p}^\rho \equiv 0(\mathfrak{q}). \tag{15.6}$$

使得这个关系成立的最小数 ρ 叫做 $\mathfrak{q}$ 的指数. 特别, 这个指数给出为了使 $\mathfrak{p}$ 的元素幂属于 $\mathfrak{q}$ 所需要的最小乘方指数的上界.

若 $\mathfrak{q}$ 是准素的, 那么方程 (15.6) 对属于 $\mathfrak{q}$ 的素理想 $\mathfrak{p}$ 来说是一个特征性质. 因为假定有第二个素理想 $\mathfrak{p}'$ 带有指数 ρ' 同样也满足 (15.6), 那么将有

$$\mathfrak{p}^\rho \subseteq \mathfrak{q} \subseteq \mathfrak{p}', \quad \text{从而 } \mathfrak{p} \subseteq \mathfrak{p}',$$

$$\mathfrak{p}'^{\rho'} \subseteq \mathfrak{q} \subseteq \mathfrak{p}, \quad 从而\ \mathfrak{p}' \subseteq \mathfrak{p},$$

因此 $\mathfrak{p}' = \mathfrak{p}$.

定理 6　*若 $\mathfrak{ab} \equiv 0(\mathfrak{q})$, 且 $\mathfrak{q} \not\equiv 0(\mathfrak{q})$, 那么有一个幂 $\mathfrak{b}^\sigma \equiv 0(\mathfrak{q})$.*

证　只要取 $\sigma = \rho$ 即可. 正如以前所证明的那样, 由 $\mathfrak{ab} \equiv 0(\mathfrak{q})$ 及 $\mathfrak{a} \not\equiv 0(\mathfrak{q})$ 就得出 $\mathfrak{b} \equiv 0(\mathfrak{p})$, 从而

$$\mathfrak{b}^\rho \equiv 0(\mathfrak{p}^\rho) \equiv 0(\mathfrak{q}).$$

一个具有最后所说的性质的理想 $\mathfrak{q}$ 叫做*强准素的*, 它是与先前所定义的*弱准素*或简称准素理想相对的. 如果因子链条件成立, 那么这两个概念是一致的. 因为我们已经看到, 这时准素理想也是强准素的, 而通过把理想 $\mathfrak{a}, \mathfrak{b}$ 特殊化为主理想 $(a), (b)$, 就可以简单地推出其逆. 如果因子链条件不成立, 那么虽然每一个强准素理想也是弱准素的, 然而反过来不一定成立. 请看在*Math. Reviews,* 1944, 5:226 上关于 Walfisch A. “Über primäre Ideale”的文摘.

习题 15.3　在一个不定元 x 的整系数多项式环中, 理想 $\mathfrak{a} = (x^2, 2x)$ 不是准素的. 然而 $(x)^2 \subset \mathfrak{a} \subset (x)$, 而 (x) 是一个素理想.

习题 15.4　若 $\mathfrak{o}$ 有单位元, 那么 $\mathfrak{o}$ 本身是属于素理想 $\mathfrak{o}$ 的唯一准素理想.

15.4　一般分解定理

从现在起, 设 $\mathfrak{o}$ 是一个 Noether 环. 因此在 $\mathfrak{a}$ 中基条件、因子链条件、极大条件以及因子归纳原理成立.

一个理想 $\mathfrak{m}$ 叫做*可约的*, 如果它可以被表示成两个真因子的交:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \quad \mathfrak{a} \supset \mathfrak{m}, \quad \mathfrak{b} \supset \mathfrak{m}.$$

如果这样的表示不可能, 那么就说这个理想*不可约*.

素理想是不可约理想的例子, 因为如果一个素理想 $\mathfrak{p}$ 可以表示为

$$\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}, \quad \mathfrak{a} \supset \mathfrak{p}, \quad \mathfrak{b} \supset \mathfrak{p},$$

那么将有

$$\mathfrak{ab} \equiv 0(\mathfrak{a} \cap \mathfrak{b}) \equiv 0(\mathfrak{p}), \quad \mathfrak{a} \not\equiv 0(\mathfrak{p}), \quad \mathfrak{b} \not\equiv 0(\mathfrak{p}),$$

这与素理想的性质相违.

根据因子链条件, 以下的*第一分解定理*成立:

第一分解定理　*每一个理想都是有限个不可约理想的交.*

证　对于不可约理想来说, 定理正确. 设 $\mathfrak{m}$ 可约:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \quad \mathfrak{a} \supset \mathfrak{m}, \quad \mathfrak{b} \supset \mathfrak{m}.$$

假定对于 $\mathfrak{m}$ 的一切真因子, 因而特别对于 $\mathfrak{a}$ 及 $\mathfrak{b}$ 来说, 定理已被证明. 于是可以设

$$\mathfrak{a} = [\mathfrak{i}_1, \cdots, \mathfrak{i}_s],$$
$$\mathfrak{b} = [\mathfrak{i}_{s+1}, \cdots, \mathfrak{i}_r].$$

然而, 由此就得出

$$\mathfrak{m} = [\mathfrak{i}_1, \cdots, \mathfrak{i}_s, \mathfrak{i}_{s+1}, \cdots, \mathfrak{i}_r].$$

所以定理对于 $\mathfrak{m}$ 也成立. 然而定理对于单位理想 (总是不可约的) 成立, 于是根据 "因子归纳原理", 定理一般成立.

利用下面的定理, 可以由不可约理想表示出发, 得出准素理想表示:

定理　*每一个不可约理想都是准素的.*

证　设 $\mathfrak{m}$ 不是准素的. 我们将证明, $\mathfrak{m}$ 可约. 因为 $\mathfrak{m}$ 不准素, 所以存在两个元素 a, b 具有性质

$$ab \equiv 0(\mathfrak{m}),$$
$$a \not\equiv 0(\mathfrak{m}),$$
$$b^\rho \not\equiv 0(\mathfrak{m}) \quad 对任意\rho.$$

根据因子链条件, 理想商的序列

$$\mathfrak{m} : b, \mathfrak{m} : b^2, \cdots$$

在某一项终止, 换一句话说, 对于某一 k,

$$\mathfrak{m} : b^k = \mathfrak{m} : b^{k+1}.$$

我们现在断言,

$$\mathfrak{m} = (\mathfrak{m}, a) \cap (\mathfrak{m}, \mathfrak{o}b^k). \tag{15.7}$$

右端两个理想都是 $\mathfrak{m}$ 的因子, 并且还是真因子, 因为第一个包含 a, 第二个包含 b^{k+1}. 我们需要证明, 这两个理想的任意公共元素必定属于 $\mathfrak{m}$. 一个这样的元素 c, 作为 $(\mathfrak{m}, \mathfrak{o}b^k)$ 的元素, 具有形式

$$c = m + rb^k.$$

其次, 作为 $(\mathfrak{m}, a)$ 的一个元素, 它具有性质

$$cb \equiv 0(\mathfrak{m}b, ab) \equiv 0(\mathfrak{m}).$$

由此推出

$$mb + rb^{k+1} = cb \equiv 0(\mathfrak{m}),$$
$$rb^{k+1} \equiv 0(\mathfrak{m}).$$

从而根据 $\mathfrak{m} : b^{k+1} = \mathfrak{m} : b^k$, 有

$$rb^k \equiv 0(\mathfrak{m}),$$
$$c = m + rb^k \equiv 0(\mathfrak{m}).$$

于是 (15.7) 被证明. 所以 $\mathfrak{m}$ 的确是可约的.

因为每一理想都可以被表示成有限个不可约理想的交, 而每一不可约理想都是准素的, 所以

定理　*每一理想都可以被表示成有限个准素理想的交.*

这个定理还可以再加强. 首先从一个表示

$$\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r]$$

里可以依次将多余的理想 $\mathfrak{q}_i$, 也就是一切包含其余理想的交的理想去掉. 于是得到一个不可缩短的表示, 就是这样的一个表示, 在其中每一成分 $\mathfrak{q}_i$ 都不再包有其余成分的交. 在这样的一个表示里, 还可以发现, 一些准素成分可能括成一个准素理想, 也就是说, 它们的交仍是一个准素理想. 什么时候才会发生这种情形, 由以下定理给出.

定理 1　*有限个属于同一素理想的准素理想的交仍是一个准素理想, 并且属于同一素理想.*

定理 2　*有限个准素理想, 如果不都属于同一素理想, 那么它们的不可缩短的交不是准素的.*

这个定理不依赖于因子链条件.

定理 1 的证明　设

$$\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r],$$

此处 $\mathfrak{q}_1, \cdots, \mathfrak{q}_r$ 都属于 $\mathfrak{p}$. 我们根据定理 3 (15.3 节) 来证明. 由

$$ab \equiv 0(\mathfrak{m}), \quad a \not\equiv 0(\mathfrak{m})$$

推出, 对于一切 ν,

$$ab \equiv 0(\mathfrak{q}_\nu),$$

并且至少对于一个 ν,

$$a \not\equiv 0(\mathfrak{q}_\nu),$$

从而

$$b \equiv 0(\mathfrak{p}).$$

其次, 显然有

$$\mathfrak{m} \equiv 0(\mathfrak{q}_\nu) \equiv 0(\mathfrak{p}).$$

最后, 若 $b \equiv 0(\mathfrak{p})$ 那么对一切 ν,

$$b^{\rho_\nu} \equiv 0(\mathfrak{q}_\nu),$$

因此, 当 $\rho = \max \rho_\nu$ 时, 有

$$\begin{aligned} &b^\rho \equiv 0(\mathfrak{q}_\nu) \quad \text{对一切}\nu, \\ &b^\rho \equiv 0(\mathfrak{m}). \end{aligned}$$

于是, 定理 3 (15.3 节) 所说的三个性质都被满足. 因此 $\mathfrak{m}$ 是准素的而 $\mathfrak{p}$ 是属于它的素理想.

定理 2 的证明 设给定一个不可缩短表示

$$\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r] \quad (r \geqslant 2),$$

在其中所属的素理想 $\mathfrak{p}_\nu$ 至少有两个不相同. 我们一开始就设想每一组属于同一素理想的准素理想都括成了一个准素理想. 这个表示仍是不可缩短的.

在有限个素理想 $\mathfrak{p}_\nu$ 中存在一个极小的素理想, 就是这样的一个素理想, 它不包含同组中其他任何一个. 例如, 设这个素理想是 $\mathfrak{p}_1$. 因为 $\mathfrak{p}_1$ 不包含 $\mathfrak{p}_2, \cdots, \mathfrak{p}_r$, 所以有元素 a_ν 使得

$$\left.\begin{aligned} a_\nu \not\equiv 0(\mathfrak{p}_1), \\ a_\nu \equiv 0(\mathfrak{p}_\nu), \end{aligned}\right\} \quad (\nu = 2, 3, \cdots, r).$$

因此, 对于充分大的 ρ,

$$a_\nu^\rho \equiv 0(\mathfrak{q}_\nu).$$

如果 $\mathfrak{q}_1 = \mathfrak{m}$, 那么表示 $\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r]$ 可以缩短 (这时 $\mathfrak{q}_2, \cdots, \mathfrak{q}_r$ 是多余的). 因此, 在 $\mathfrak{q}_1$ 里存在一个元素 q_1 使得

$$q_1 \not\equiv 0(\mathfrak{m}).$$

这时, 积

$$q_1(a_2 \cdots a_r)^\rho$$

属于 $\mathfrak{q}_1$ 且同时属于 $\mathfrak{q}_2, \cdots, \mathfrak{q}_r$, 从而属于 $\mathfrak{m}$. 然而 q_1 不属于 $\mathfrak{m}$. 如果 $\mathfrak{m}$ 是准素的, 那么由此将推出

$$(a_2 \cdots a_r)^{\rho\sigma} \equiv 0(\mathfrak{m}),$$

$$(a_2 \cdots a_r)^{\rho\sigma} \equiv 0(\mathfrak{p}_1),$$

于是, 因为 $\mathfrak{p}_1$ 是素理想, 至少对于一个 ν,

$$a_\nu \equiv 0(\mathfrak{p}_1),$$

这与前面所说的矛盾.

如果在一个不可缩短表示

$$\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r]$$

里, 属于 $\mathfrak{q}_\nu$ 的素理想 $\mathfrak{p}_\nu$ 都互不相同, 这时表示里两个或几个理想都无法括成一个素理想, 那么这个表示就叫做一个*由最大准素理想的表示*. 这些最大准素理想也叫做 $\mathfrak{m}$ 的*准素分支*.

每一个不可缩短表示 $\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r]$ 都可以通过把属于同一素理想的准素理想括在一起而化为一个由最大准素理想的表示. 于是就证明了

第二分解定理 *每一理想都容许一个被表成有限个最大准素分支的交的不可缩短表示. 这些准素分支属于互不相同的素理想.*

由 Lasker 对多项式环而由 Noether 对一般环所证明的“第二分解定理”是一般理想论中最重要的结果. 我们将在整个第 16 章中看到这个定理的应用. 在下一节里我们将研究准素分支的唯一性问题.

习题 15.5 在一个不定元的整系数多项式环内把理想 $(9, 3x+3)$ 分解为准素分支.

习题 15.6 对于每一理想 $\mathfrak{a}$, 存在一个可以被 $\mathfrak{a}$ 整除的素理想幂的积 $\mathfrak{p}_1^{\rho_1} \cdot \mathfrak{p}_2^{\rho_2} \cdots \mathfrak{p}_h^{\rho_h}$, 其中每一 $\mathfrak{p}_\nu$ 都是 $\mathfrak{a}$ 的一个因子.

习题 15.7 若环 $\mathfrak{o}$ 有单位元, 那么每一个异于 $\mathfrak{o}$ 的理想 $\mathfrak{a}$ 至少可以被一个异于 $\mathfrak{o}$ 的素理想整除.

习题 15.8 在一个不定元的整系数多项式环内, 理想 $(4, 2x, x^2)$ 是准素的, 但是可约的 (分解：$(4, 2x, x^2) = (4, x) \cap (2, x^2)$).

15.5 第一唯一性定理

一个理想分成最大准素分支的分解不是唯一的.

例 在多项式环 $K(x, y)$ 里, 理想

$$\mathfrak{m} = (x^2, xy)$$

由一切可以被 x 整除且不含一次项的多项式组成. 一切可以被 x 整除的多项式的集是素理想

$$\mathfrak{q}_1=(x).$$

一切不含一次项及常数项的多项式的集是准素理想

$$\mathfrak{q}_2=(x^2,xy,y^2).$$

因此

$$\mathfrak{m}=[\mathfrak{q}_1,\mathfrak{q}_2].$$

这是一个不可缩短表示, 并且由于属于 $\mathfrak{q}_1$ 与 $\mathfrak{q}_2$ 的素理想不相同, 它们分别是 (x) 及 (x,y), 所以这也是一个由最大准素理想的表示.

然而, 除此之外还有另外的表示:

$$\mathfrak{m}=[\mathfrak{q}_1,\mathfrak{q}_3],$$

这里

$$\mathfrak{q}_3=(x^2,y).$$

因为一个多项式属于 $\mathfrak{m}$, 只要求它可以被 x 整除并且不含有一次项就行. 按这种方法, 当域 K 是无限的时候, 甚至有无限多种表示:

$$\mathfrak{m}=[\mathfrak{q}_1,\mathfrak{q}^{(\lambda)}],\quad \mathfrak{q}^{(\lambda)}=(x^2,y+\lambda x).$$

在所求得的 $\mathfrak{m}$ 的一切分解中, 准素分支的 $\mathfrak{q}$个数以及所属的素理想

$$(x),\quad (x,y)$$

都是唯一确定的. 一般来说, 以下定理成立:

第一唯一性定理 *在一个理想 $\mathfrak{m}$ 用最大准素分支的两种不可缩短表示中, 分支的个数以及所属的素理想都是唯一确定的 (尽管分支本身不见得唯一确定).*

证 对于一个准素理想来说, 断言是自明的. 因此, 可以对于出现在所考虑的理想的至少一个表示内的准素分支的个数作归纳法. 设

$$\mathfrak{m}=[\mathfrak{q}_1,\cdots,\mathfrak{q}_l]=[\mathfrak{q}'_1,\cdots,\mathfrak{q}'_{l'}].\tag{15.8}$$

从一切所属的素理想 $\mathfrak{p}_1,\cdots,\mathfrak{p}_l,\mathfrak{p}'_1,\cdots,\mathfrak{p}'_{l'}$ 中选出一个极大的, 就是这样的一个素理想, 它不被其余任何一个所包含 (整除). 例如, 设这样的一个理想出现在 (15.8) 的左端, 并且设它为 $\mathfrak{p}_1$. 我们断言, 这个理想也出现在右端. 因为不然的话, 我们可以在 (15.8) 里作对于 $\mathfrak{q}_1$ 的商:

$$[\mathfrak{q}_1:\mathfrak{q}_1,\cdots,\mathfrak{q}_l:\mathfrak{q}_1]=[\mathfrak{q}'_1,:\mathfrak{q}_1,\cdots,\mathfrak{q}'_{l'}:\mathfrak{q}_1].$$

现在 (对于一切 $\nu > 1$)$\mathfrak{q}_1 \not\equiv 0(\mathfrak{p}_\nu)$, 否则将有 $\mathfrak{p}_1 \equiv 0(\mathfrak{p}_\nu)$, 这与 $\mathfrak{p}_1$ 的极大性的假设相违. 同理, 对于一切 $\nu, \mathfrak{q}_1 \not\equiv 0(\mathfrak{p}'_\nu)$. 于是根据定理 4′(15.3 节),

$$\mathfrak{q}_\nu : \mathfrak{q}_1 = \mathfrak{q}_\nu \quad (\nu = 2, \cdots, l),$$

$$\mathfrak{q}'_\nu : \mathfrak{q}_1 = \mathfrak{q}'_\nu \quad (\nu = 1, \cdots, l').$$

然而 $\mathfrak{q}_1 : \mathfrak{q}_1 = \mathfrak{o}$, 所以有

$$[\mathfrak{o}, \mathfrak{q}_2, \cdots, \mathfrak{q}_l] = [\mathfrak{q}'_1, \cdots, \mathfrak{q}'_{l'}].$$

右端等于 $\mathfrak{m}$. 所以左端也必须等于 $\mathfrak{m}$. $\mathfrak{o}$ 可以去掉. 所以

$$\mathfrak{m} = [\mathfrak{q}_2, \cdots, \mathfrak{q}_l].$$

于是, (15.8) 中两个表示的第一个可以缩短, 与假设矛盾.

这样, 每一个极大素理想都在两端出现.

现在设, 例如, $l \leqslant l'$. 我们要证明：$l = l'$ 并且 (适当排列次序) $\mathfrak{p}_\nu = \mathfrak{p}'_\nu$. 假设这个结论对于可以用少于 l 个准素理想表示的理想来说, 已完全被证明. 我们如此排列 $\mathfrak{q}$ 与 $\mathfrak{q}'$ 的次序使得 $\mathfrak{p}_1 = \mathfrak{p}'_1$ 是属于 $\mathfrak{q}_1$ 及 $\mathfrak{q}'_1$ 的极大素理想.

在 (15.8) 的两端作对于积 $\mathfrak{q}_1\mathfrak{q}'_1$ 的商：

$$[\mathfrak{q}_1 : \mathfrak{q}_1\mathfrak{q}'_1, \cdots, \mathfrak{q}_l : \mathfrak{q}_1\mathfrak{q}'_1] = [\mathfrak{q}'_1 : \mathfrak{q}_1\mathfrak{q}'_1, \cdots, \mathfrak{q}'_1 : \mathfrak{q}_1\mathfrak{q}'_1],$$

于是按照与前面同样的论证得

$$\left.\begin{array}{l} \mathfrak{q}_\nu : \mathfrak{q}_1\mathfrak{q}'_1 = \mathfrak{q}_\nu \\ \mathfrak{q}'_\nu : \mathfrak{q}_1\mathfrak{q}'_1 = \mathfrak{q}'_\nu \end{array}\right\} (\nu > 1).$$

再者, 因为 $\mathfrak{q}_1\mathfrak{q}'_1$ 能被 $\mathfrak{q}_1$ 及 $\mathfrak{q}'_1$ 整除, 所以

$$\mathfrak{q}_1 : \mathfrak{q}_1\mathfrak{q}'_1 = \mathfrak{o},$$

$$\mathfrak{q}'_1 : \mathfrak{q}_1\mathfrak{q}'_1 = \mathfrak{o}.$$

于是得到

$$[\mathfrak{q}_2, \cdots, \mathfrak{q}_l] = [\mathfrak{q}'_2, \cdots, \mathfrak{q}'_{l'}].$$

根据归纳假定, 因为现在左端和右端都是一个由最大准素分支的不可缩短表示, $l' - 1 = l - 1$, 从而 $l' = l$. 其次, 适当排列次序, 对一切 $\nu > 1, \mathfrak{p}_\nu = \mathfrak{p}'_\nu$ 成立. 此外, 因为 $\mathfrak{p}_1 = \mathfrak{p}'_1$, 所以定理完全被证明.

按照所证的定理, 作为所属素理想而出现在一个不可缩短表示 $\mathfrak{a}=[\mathfrak{q}_1,\cdots,\mathfrak{q}_l]$ 中的唯一确定的理想 $\mathfrak{p}_1,\cdots,\mathfrak{p}_l$ 叫做属于理想 $\mathfrak{a}$ 的素理想. 它们最重要的性质是:

当一个理想 $\mathfrak{a}$ 不能被属于一个理想 $\mathfrak{b}$ 的任何素理想整除时, 那么 $\mathfrak{b}:\mathfrak{a}=\mathfrak{b}$. 反过来也成立.

证　设 $\mathfrak{b}=[\mathfrak{q}_1,\cdots,\mathfrak{q}_l]$ 是一个不可缩短表示. 首先设 $\mathfrak{a}\not\equiv 0(\mathfrak{p}_i), i=1,\cdots,l$, 这里 $\mathfrak{p}_i$ 属于 $\mathfrak{q}_i$. 由此推出

$$\begin{aligned}\mathfrak{q}_i:\mathfrak{a}&=\mathfrak{q}_i,\\ \mathfrak{b}:\mathfrak{a}&=[\mathfrak{q}_1,\cdots,\mathfrak{q}_l]:\mathfrak{a}\\ &=[\mathfrak{q}_1:\mathfrak{a},\cdots,\mathfrak{q}_l:\mathfrak{a}]\\ &=[\mathfrak{q}_1,\cdots,\mathfrak{q}_l]=\mathfrak{b}.\end{aligned}$$

反过来, 设 $\mathfrak{b}:\mathfrak{a}=\mathfrak{b}$. 如果对于某一 $i, \mathfrak{a}\equiv 0(\mathfrak{p}_i)$, 例如 $\mathfrak{a}\equiv 0(\mathfrak{p}_1)$, 那么将有 $\mathfrak{a}^\rho\equiv 0(\mathfrak{q}_1)$, 从而

$$\mathfrak{a}^\rho\cdot[\mathfrak{q}_2,\cdots,\mathfrak{q}_l]\equiv 0([\mathfrak{q}_1,\cdots,\mathfrak{q}_l])\equiv 0(\mathfrak{b}).$$

因为在每一同余式 (mod $\mathfrak{b}$) 里可以约去 $\mathfrak{a}$, 因而可以约去 $\mathfrak{a}^\rho$, 所以

$$[\mathfrak{q}_2,\cdots,\mathfrak{q}_l]\equiv 0(\mathfrak{b}),$$

这与表示的不可缩短性相违.

特别, 当 $\mathfrak{a}$ 是一个主理想 (a) 时, 我们得到一个重要的特殊情形:

当一个元素 a 不能被属于一个理想 $\mathfrak{b}$ 的任何素理想整除时, 那么 $\mathfrak{b}:a=\mathfrak{b}$. 这就是说, 由 $ac\equiv 0(\mathfrak{b})$ 推出 $c\equiv 0(\mathfrak{b})$.

当把 $\mathfrak{a}$ 也表示成准素理想的交 $[\mathfrak{q}'_1,\cdots,\mathfrak{q}'_{l'}]$ 时, 我们还可以用另外方式来陈述这个一般定理. $\mathfrak{a}$ 可以被 $\mathfrak{p}_i$ 整除, 当且仅当某一 $\mathfrak{q}'_j$ 能被 $\mathfrak{p}_i$ 整除, 即某一 $\mathfrak{p}'_j$ 能被 $\mathfrak{p}_i$ 整除. 由此推出:

当属于 $\mathfrak{a}$ 的任何一个素理想都不能被属于 $\mathfrak{b}$ 的一个素理想整除时, $\mathfrak{b}:\mathfrak{a}=\mathfrak{b}$. 反过来也成立.

15.6　孤立分支与符号幂

在一个交换环 $\mathfrak{o}$ 里, 设 S 是一个非空集, 它在含有两个元素 s 与 t 的同时也含有它们的积 st. 这样的一个集 S 叫做乘法封闭的.

现在设 $\mathfrak{m}$ 是 $\mathfrak{o}$ 的一个理想. 我们将 $\mathfrak{m}_S$ 理解为 $\mathfrak{o}$ 中一切这样的元素 x 的集, 对于 S 的一个 s, sx 属于 $\mathfrak{m}$.

$\mathfrak{m}_S$ 是一个理想 (并且还是 $\mathfrak{m}$ 的一个因子). 当 x 与 y 属于 $\mathfrak{m}_S$ 时, sx 与 $s'y$ 属于 $\mathfrak{m}$, 因而

$$ss'(x-y) = s'(sx) - s(s'y)$$

也属于 $\mathfrak{m}$, 所以 $x-y$ 属于 $\mathfrak{m}_S$; 当 x 属于 $\mathfrak{m}_S$ 时, rx 也属于 $\mathfrak{m}_S$. 至于 $\mathfrak{m}$ 的一切元素都属于 $\mathfrak{m}_S$, 显然.

$\mathfrak{m}_S$ 叫做 $\mathfrak{m}$ 的 *S分支*, 或者更详细地说, 叫做*由 S 所确定的 $\mathfrak{m}$ 的孤立分支*.

从现在起, 再假设 $\mathfrak{o}$ 是一个 Noether 环. 如果理想 $\mathfrak{m}$ 被表示成准素理想的交:

$$\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r], \tag{15.9}$$

那么可以将准素理想 $\mathfrak{q}_i$ 区分为与 S 相遇的, 就是至少与 S 有一个公共元素, 和不与 s 相遇的. 如果一个 $\mathfrak{q}_i$ 与 S 有一个公共元素 s, 那么属于 $\mathfrak{q}_i$ 的素理想 $\mathfrak{p}_i$ 也与 S 有同一公共元素 s. 反过来, 如果 $\mathfrak{p}_i$ 与 S 有一个公共元素 s, 那么 $\mathfrak{q}_i$ 有一个幂 s^ρ 与 S 公共.

我们将 $\mathfrak{q}_i$ 这样编号, 使得 $\mathfrak{q}_1, \cdots, \mathfrak{q}_h$ 不与集 S 相遇, 而 $\mathfrak{q}_{k+1}, \cdots, \mathfrak{q}_r$ 与 S 相遇. 我们现在证明,

$$\mathfrak{m}_S = [\mathfrak{q}_1, \cdots, \mathfrak{q}_h]. \tag{15.10}$$

在 $h=0$ 的情形, (15.10) 就意味着 $\mathfrak{m}_S = \mathfrak{o}$.

证 如果 x 属于 $\mathfrak{m}_S$, 那么 sx 属于 $\mathfrak{m}$, 于是, 对于 $1 \leqslant i \leqslant h$, 有

$$sx \equiv 0(\mathfrak{q}_i), \quad s \not\equiv 0(\mathfrak{p}_i), \quad \text{从而} x \equiv 0(\mathfrak{q}_i),$$

换句话说, x 属于 $[\mathfrak{q}_1, \cdots, \mathfrak{q}_h]$. 反过来, 若 x 属于 $[\mathfrak{q}_1, \cdots, \mathfrak{q}_h]$, 那么在 $r > h$ 的情形下, 可以对于从 $h+1$ 到 r 的每一个 i 在 S 中选出一个 s_i, 使得它能被 $\mathfrak{q}_i$ 整除. 现在, 令

$$s = s_{h+1} \cdots s_r.$$

在 $r = h$ 的情形, 我们在 S 里选任意一个 s. 在两种情形 sx 都能被 $\mathfrak{q}_i$ 整除, 即 sx 属于 $\mathfrak{m}$, 从而 x 属于 $\mathfrak{m}_S$.

$\mathfrak{m}$ 的一个准素分支 $\mathfrak{q}_i$ 叫做*嵌入的*, 假如属于它的素理想 $\mathfrak{p}_i$ 是属于 $\mathfrak{m}$ 的另一素理想 $\mathfrak{p}_j$ 的因子, 相反地, 如果不是这种情形, 就叫做*孤立的*. 在第一种情形, 属于它的素理想 $\mathfrak{p}_i$ 也叫做*嵌入的*(且嵌入 $\mathfrak{p}_j$), 在第二种情形就叫做*孤立的*. 同样, 一切 $\mathfrak{q}_i$ 的集的一个子集 $\{\mathfrak{q}_a, \mathfrak{q}_b, \cdots\}$, 或相应地, 一切 $\mathfrak{p}_i$ 的集的子集 $\{\mathfrak{p}_a, \mathfrak{p}_b, \cdots\}$ 叫做*孤立的*, 假如这个子集的任何 $\mathfrak{p}_i$ 都不是一个不属于这个子集的 $\mathfrak{p}_i$ 的因子.

当 $\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r]$ 时, 对于每一乘法封闭集 S, 都有一个由那些不含 S 的元素的 $\mathfrak{p}_i$ 所组成的孤立子集 $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_h\}$ 与它相应. 这个子集是孤立的, 因为若 $\mathfrak{p}_i$ 属

于这个子集并且是 $\mathfrak{p}_j$ 的一个因子, 那么 $\mathfrak{p}_j$ 也属于这个子集. 于是属于 $\mathfrak{p}_1, \cdots, \mathfrak{p}_h$ 的准素理想 $\mathfrak{q}_1, \cdots, \mathfrak{q}_h$ 的交就是孤立分支 $\mathfrak{m}_S$.

如果选出一个孤立的 $\mathfrak{p}_i$, 并且选取 $\mathfrak{o}$ 中不能被 $\mathfrak{p}_i$ 整除的元素所成的集作为 S, 那么就得到一个重要的特殊情形. 除去不感兴趣的情形 $\mathfrak{m} = \mathfrak{o}$ 外, 这个集是非空的. 其他每一 $\mathfrak{p}_j$ 都含有一个不能被 $\mathfrak{p}_i$ 整除的元素, 从而含有 S 的一个元素. 于是由 (15.10) 得

$$\mathfrak{m}_S = \mathfrak{q}_i.$$

现在 $\mathfrak{m}_S$ 由 $\mathfrak{m}$ 及 S, 从而由 $\mathfrak{m}$ 及 $\mathfrak{p}_i$ 唯一确定. 另一方面, 孤立的 $\mathfrak{p}_i$ 由 $\mathfrak{m}$ 唯一确定. 于是得

(15.9) 中的孤立准素分支是唯一确定的.

习题 15.9　用同样的方法证明**第二唯一性定理**: 理想 $\mathfrak{m}$ 的一个准素分支的孤立集的交 $[\mathfrak{q}_a, \mathfrak{q}_b, \cdots]$ 由所属的素理想 $\mathfrak{p}_a, \mathfrak{p}_b, \cdots$ 的给出而唯一确定.

符号幂

在 15.3 节我们已经看到, 一个素理想 $\mathfrak{p}$ 的幂 $\mathfrak{p}^r$ 不一定是准素的. 将 $\mathfrak{p}^r$ 表示成准素分支的交:

$$\mathfrak{p}^r = [\mathfrak{q}_1, \cdots, \mathfrak{q}_s],$$

那么属于这些准素分支的素理想 $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ 都是 $\mathfrak{p}^r$ 的因子, 从而也都是 $\mathfrak{p}$ 的因子. 作出积 $\mathfrak{p}_1 \cdots \mathfrak{p}_s$, 于是这个积的一个幂可以被一切 $\mathfrak{q}_i$, 从而被 $\mathfrak{p}^r$, 从而被 $\mathfrak{p}$ 整除. 所以因子之一, 例如 $\mathfrak{p}_1$, 必须能被 $\mathfrak{p}$ 整除. 另一方面, $\mathfrak{p}_1$ 是 $\mathfrak{p}$ 的一个因子, 所以 $\mathfrak{p}_1 = \mathfrak{p}$.

其余的 $\mathfrak{p}_i (i \neq 1)$ 都是 $\mathfrak{p}$ 的真因子. 由此得出, $\mathfrak{q}_1$ 是 $\mathfrak{p}^r$ 的一个孤立准素分支, 从而是唯一确定的. $\mathfrak{q}_1$ 正是由 S 所确定的 $\mathfrak{p}^r$ 的孤立分支 $\mathfrak{p}^r_S$, 这里 S 是 $\mathfrak{o}$ 中一切不能被 $\mathfrak{p}$ 整除的元素的集.

这样唯一确定的 $\mathfrak{p}^r$ 的属于素理想 $\mathfrak{p}_1 = \mathfrak{p}$ 的准素分支, 依照 Krull 的说法, 叫做 $\mathfrak{p}$ 的 r *次符号幂*, 并且记作 $\mathfrak{p}^{(r)}$.

15.7　无公因子的理想论

以下将假设在环 $\mathfrak{o}$ 里单位元存在. 于是, 这个单位元生成单位理想 $\mathfrak{o}$:

$$\mathfrak{o} = (1).$$

两个理想 $\mathfrak{a}, \mathfrak{b}$ 叫做*无公因子的*, 假如它们除 $\mathfrak{o}$ 外没有任何公因子, 换句话说, 它们的最大公因子是 $\mathfrak{o}$:

$$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}.$$

这就意味着 $\mathfrak{o}$ 的每一元素可以被表示成 $\mathfrak{a}$ 的一个元素与 $\mathfrak{b}$ 的一个元素的和.

对此必要且只要单位元 ($\mathfrak{o}$ 的生成元) 可以被表示成和：

$$1 = a + b \tag{15.11}$$

(a 属于 $\mathfrak{a}, b$ 属于 $\mathfrak{b}$). 于是有

$$\begin{aligned} a \equiv 1(\mathfrak{b}), \quad b \equiv 0(\mathfrak{b}), \\ a \equiv 0(\mathfrak{a}), \quad b \equiv 1(\mathfrak{a}). \end{aligned} \tag{15.12}$$

如果两个准素理想 $\mathfrak{q}_1, \mathfrak{q}_2$ 无公因子, 那么属于它们的素理想 $\mathfrak{p}_1, \mathfrak{p}_2$ 更是如此 ($\mathfrak{p}_1$ 与 $\mathfrak{p}_2$ 的每一公因子也是 $\mathfrak{q}_1$ 与 $\mathfrak{q}_2$ 的一个公因子). 反过来也成立：*若 $\mathfrak{p}_1$ 与 $\mathfrak{p}_2$ 无公因子, 则 $\mathfrak{q}_1$ 与 $\mathfrak{q}_2$ 也无公因子*. 因为由

$$1 = p_1 + p_2$$

自乘 $(\rho + \sigma - 1)$ 次方得

$$1 = p_1^{\rho+\sigma-1} + \cdots + p_2^{\rho+\sigma-1}.$$

现在将 ρ 与 σ 选得如此之大, 使得 p_1^ρ 属于 $\mathfrak{q}_1$ 且 p_2^σ 属于 $\mathfrak{q}_2$, 那么右端的和里每一项或者属于 $\mathfrak{q}_1$ 或者属于 $\mathfrak{q}_2$, 从而

$$1 \in \mathfrak{q}_1 + \mathfrak{q}_2.$$

定理　*如果两个理想 $\mathfrak{a}$ 和 $\mathfrak{b}$ 无公因子, 那么 $\mathfrak{a} : \mathfrak{b} = \mathfrak{a}$ 且 $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$.*

证　设 $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$, 于是 $a + b = 1$. 只需证明 $\mathfrak{a} : \mathfrak{b} \subseteq \mathfrak{a}$. 若 x 属于 $\mathfrak{a} : \mathfrak{b}$, 则 $x\mathfrak{b} \subseteq \mathfrak{a}$, 于是 $xb \equiv 0(\mathfrak{a})$, 从而也有

$$\begin{aligned} x(a+b) &\equiv 0(\mathfrak{a}), \\ x \cdot 1 &\equiv 0(\mathfrak{a}). \end{aligned}$$

因此 x 属于 $\mathfrak{a}$. 证毕.

命题的反面不成立. 例如, 在多项式环 $K[x, y]$ 里, 理想 (x) 与 (y) 是彼此互素的 (两个理想 $\mathfrak{a}$ 和 $\mathfrak{b}$ 称为彼此*互素*的, 如果属于一个理想的任一素理想都不整除另一个理想, 亦即上定理的结合成立 (参见 14.5 节)), 然而不是无公因子的：

$$(x, y) \neq \mathfrak{o},$$

$$\begin{cases} (x) : (y) = (x), \\ (y) : (x) = (y). \end{cases}$$

当 $\mathfrak{a}$ 与 $\mathfrak{b}$ 无公因子时, 我们可以像数论里那样来解联立同余式. 设给定两个同余式

$$f(\xi) \equiv 0(\mathfrak{a}),$$
$$g(\xi) \equiv 0(\mathfrak{b}) \quad (f(x), g(x) \in \mathfrak{o}(x)).$$

假定每一个单独的同余式都是可解的. 设 $\xi \equiv \alpha$ 是第一个同余式的一个解, $\xi = \beta$ 是第二个同余式的一个解, 那么可以按以下方法求得一个元素 ξ, 使得两个同余式都被解出：利用以前所作的满足方程 (15.11) 和 (15.12) 的元素 a, b, 我们作

$$\xi = b\alpha + a\beta.$$

因为 $\xi \equiv \alpha(\mathfrak{a})$ 且 $\xi \equiv \beta(\mathfrak{b})$, 所以 ξ 是所给的两个同余式的一个解.

定理　两个无公因子的理想的最小公倍等于它们的积.

证　在 15.2 节里已经证明了：

$$\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b},$$

$$[\mathfrak{a} \cap \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b}) \subseteq \mathfrak{ab}.$$

现在, 如果 $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ 并且有单位元存在, 那么第二个方程可以简化为

$$a \cap \mathfrak{b} \subseteq \mathfrak{ab}.$$

从而

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}.$$

为了对于多于两个的两两无公因子的理想也能叙述这个定理, 我们需要先讲一个引理.

引理　如果 $\mathfrak{a}$ 与 $\mathfrak{b}$ 和 $\mathfrak{c}$ 都没有公因子, 那么 $\mathfrak{a}$ 与积 $\mathfrak{bc}$ 以及交 $\mathfrak{b} \cap \mathfrak{c}$ 也没有公因子.

证　由

$$a + b = 1,$$
$$a' + c = 1$$

得出

$$(a + b)(a' + c) = 1,$$

$$aa' + ac + a'b + bc = 1,$$

$$a'' + bc = 1,$$

这里 $a'' = aa' + ac + a'b$ 仍是 $\mathfrak{a}$ 的一个元素. 由此推出

$$(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = \mathfrak{o},$$

因而更有

$$(\mathfrak{a}, \mathfrak{b} \cap \mathfrak{c}) = \mathfrak{o}.$$

于是两个论断都被证明.

现在设 $\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_n$ 是两两无公因子的理想, 且设

$$[\mathfrak{b}_1, \cdots, \mathfrak{b}_{n-1}] = \mathfrak{b}_1 \cdots \mathfrak{b}_{n-1}$$

已被证明, 那么

$$\begin{aligned}[\mathfrak{b}_1, \cdots, \mathfrak{b}_n] &= [\mathfrak{b}_1, \cdots, \mathfrak{b}_{n-1}] \cap \mathfrak{b}_n \\ &= (\mathfrak{b}_1, \cdots \mathfrak{b}_{n-1}) \cap \mathfrak{b}_n \\ &= \mathfrak{b}_1 \cdots \mathfrak{b}_{n-1} \cdot \mathfrak{b}_n,\end{aligned}$$

于是由归纳法得到以下定理:

定理　有限个两两无公因子的理想的最小公倍等于它们的积.

前面关于解对两个无公因子理想的同余式的注对更多的两两无公因子的理想来说也成立:

如果 $\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_r$ 是两两无公因子的理想, 那么由同余式

$$\xi \equiv \beta_i(\mathfrak{b}_i) \quad (i = 1, 2, \cdots, r)$$

总可以确定 ξ.

证　用归纳法. 如果 η 已经被确定, 使得

$$\eta \equiv \beta_i(\mathfrak{b}_i) \quad (i = 1, 2, \cdots, r-1),$$

那么 ξ 总可以由同余式

$$\begin{aligned}\xi &\equiv \eta([\mathfrak{b}_1, \cdots, \mathfrak{b}_{r-1}]), \\ \xi &\equiv \beta_r(\mathfrak{b}_r)\end{aligned}$$

定出, 因为 $\mathfrak{b}_r$ 与 $[\mathfrak{b}_1, \cdots, \mathfrak{b}_{r-1}]$ 无公因子.

定理　如果在 $\mathfrak{o}$ 里, 因子链条件成立, 那么每一个理想可以被表示成两两无公因子的理想的交, 而这些理想本身再不能被表示成两两无公因子的真因子的交.

为了这个目的, 我们在所给的理想 $\mathfrak{m}$ 的一个用准素理想的不可缩短表示

$$\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r]$$

里, 求出一切这样的准素理想, 它们与其中任意一个固定的理想通过一串非两两无公因子的准素理想联系着, 并且作一切这样理想的交 $\mathfrak{b}_1$. 按同样方式由剩下的理想中依次作理想 $\mathfrak{b}_2, \cdots, \mathfrak{b}_s$. 表示

$$\mathfrak{m} = [\mathfrak{b}_1, \cdots, \mathfrak{b}_s] \tag{15.13}$$

就具有所要求的性质. 第一, 对于任意 $i \neq k$, $\mathfrak{b}_i$ 与 $\mathfrak{b}_k$ 的确无公因子, 因为 $\mathfrak{b}_i$ 的分支与 $\mathfrak{b}_k$ 的分支无公因子. 第二, 不可能将, 例如, $\mathfrak{b}_1$ 再表示成两个彼此无公因子的真因子的交. 因为如果这样的一个表示存在:

$$\mathfrak{b}_1 = \mathfrak{b} \cap \mathfrak{c} = \mathfrak{b}\mathfrak{c},$$
$$(\mathfrak{b}, \mathfrak{c}) = \mathfrak{o},$$

那么每一个属于 $\mathfrak{b}_1$ 的素理想必定是 $\mathfrak{b}\mathfrak{c}$ 的一个因子, 从而也是 $\mathfrak{b}$ 或 $\mathfrak{c}$ 的一个因子. 现在因为一切这样的素理想都与它们之中的一个通过一串非两两无公因子的素理想联系着, 所以当其中之一能整除, 例如 $\mathfrak{b}$ 时, 一切这样的素理想都能整除 $\mathfrak{b}$ 而不能整除 $\mathfrak{c}$. 然而属于这些素理想的准素分支都整除 $\mathfrak{b}\mathfrak{c}$, 所以它们必须整除 $\mathfrak{b}$(因为它们的素理想不能整除 $\mathfrak{c}$). 于是, 交 $\mathfrak{b}_1$ 也是 $\mathfrak{b}$ 的一个因子:

$$\mathfrak{b} \subseteq \mathfrak{b}_1,$$

这与 $\mathfrak{b}$ 是 $\mathfrak{b}_1$ 的一个真因子的假设相违.

根据我们的定理, 代替表示 (15.13) 可以写出一个乘积表示:

$$\mathfrak{m} = \mathfrak{b}_1\mathfrak{b}_2\cdots\mathfrak{b}_s.$$

习题 15.10 证明: 交 (15.13) 是 13.1 节意义下的直交, 即剩余类环 $\sigma/\mathfrak{m} = \overline{\sigma}$ 是环 $\mathfrak{a}_i/\mathfrak{m} = \overline{\mathfrak{a}}_i$ 的直和, 后者同构于剩余类环 $\mathfrak{o}/\mathfrak{b}_i$(令 $\mathfrak{a}_i = [\mathfrak{b}_1, \cdots, \mathfrak{b}_{i-1}, \mathfrak{b}_{i+1}, \cdots, \mathfrak{b}_s]$, 应用 13.1 节的定理).

15.8 单素理想

仍旧设 $\mathfrak{o}$ 是一个有单位元的 Noether 环.

单位理想 $\mathfrak{o}$ 总是素理想. 什么样的准素理想可以属于这个理想? 答案是: 只有 $\mathfrak{o}$ 本身. 因为如果 $\mathfrak{q}$ 是一个属于 $\mathfrak{o}$ 的准素理想, 那么 $1 \in \mathfrak{o}$, 从而 $1^\rho \in \mathfrak{q}$, 所以 $\mathfrak{q} = \mathfrak{o}$.

在一个理想 $\mathfrak{a} \neq \mathfrak{o}$ 被表成准素理想的交的表示 $[\mathfrak{q}_1, \cdots, \mathfrak{q}_r]$ 里, 如果在所属的素理想 $\mathfrak{p}_i$ 中有单位理想出现, 那么相应的 $\mathfrak{q}_i$ 同时也等于 $\mathfrak{o}$, 从而它在这个交表示里是多余的. 因此, *如果表示 $\mathfrak{a} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r]$ 是不可缩短的且 $\mathfrak{a} \neq \mathfrak{o}$, 那么单位理想不在所属的素理想中出现.*

由此立刻推出：

每一个理想 $\mathfrak{a} \neq \mathfrak{o}$ 都至少有一个素理想因子 $\mathfrak{p} \neq \mathfrak{o}$. 如果理想 $\mathfrak{a}$ 不是准素的, 那么它至少有两个素理想因子 $\neq \mathfrak{o}$.

一个除 $\mathfrak{o}$ 外没有多于一个素理想因子的理想, 按照 Dedekind 的说法, 叫做*单素的*. 根据上面的定理, 每一个单素理想 $\mathfrak{q}$ 都是准素的. 再者, 属于它的素理想 $\mathfrak{p}$ 是极大的 (或称无因子的), 因为如果 $\mathfrak{a}' \neq \mathfrak{o}$ 是 $\mathfrak{p}$ 的一个真因子, 那么 $\mathfrak{a}'$ 将有一个素因子 $\mathfrak{p}' \neq \mathfrak{o}, \mathfrak{p}'$ 是 $\mathfrak{a}'$ 的真因子, 从而 $\mathfrak{q}$ 将有两个互不相同且异于 $\mathfrak{o}$ 的素理想因子 $\mathfrak{p}$ 与 $\mathfrak{p}'$, 这与 $\mathfrak{q}$ 的单素性的假定相违.

我们有

$$\mathfrak{p}^\rho \equiv 0(\mathfrak{q}). \tag{15.14}$$

如果 $\mathfrak{p}$ 是极大的, 那么反过来, 由关系 (15.14) 推出 $\mathfrak{q}$ 的单素性. 因为若 $\mathfrak{p}'$ 是 $\mathfrak{q}$ 的任意一个素理想的因子, 那么由 (15.14) 得

$$\mathfrak{p}^\rho \equiv 0(\mathfrak{p}'),$$

从而

$$\mathfrak{p} \equiv 0(\mathfrak{p}'),$$

于是, 或者 $\mathfrak{p}' = \mathfrak{p}$ 或者 $\mathfrak{p}' = \mathfrak{o}$. 所以 $\mathfrak{q}$ 除 $\mathfrak{p}$ 与 $\mathfrak{o}$ 外没有其他素理想因子.

这样一来, 下列概念相互等价：

(1) 单素理想;

(2) 属于一个极大素理想 $\mathfrak{p}$ 的准素理想;

(3) 一个极大素理想 $\mathfrak{p}$ 的幂 $\mathfrak{p}^\rho$ 的因子.

再者有

如果理想 $\mathfrak{m}$ 有一个孤立单素准素分支 $\mathfrak{q}$, 属于它的素理想是 $\mathfrak{p}$, 指数是 ρ, 那么对于每一整数 $\sigma \geqslant \rho$,

$$\mathfrak{q} = (\mathfrak{m}, \mathfrak{p}^\sigma). \tag{15.15}$$

证　由

$$\mathfrak{m} = 0(\mathfrak{q})$$

与

$$\mathfrak{p}^\sigma \equiv 0(\mathfrak{q})$$

得

$$(\mathfrak{m},\mathfrak{p}^{\sigma})\equiv 0(\mathfrak{q}). \tag{15.16}$$

另一方面, 设

$$\mathfrak{m}=[\mathfrak{q},\mathfrak{q}_2,\cdots,\mathfrak{q}_s]$$

是 $\mathfrak{m}$ 的一个由准素分支的表示. 理想 $(\mathfrak{m},\mathfrak{p}^{\sigma})$ 是单素的, 因而是准素的. 属于它的素理想是 $\mathfrak{p}$. 积 $\mathfrak{q}\mathfrak{q}_2\cdots\mathfrak{q}_s$ 能被 $(\mathfrak{m},\mathfrak{p}^{\sigma})$ 整除. 然而 $\mathfrak{q}_2,\cdots,\mathfrak{q}_s$ 都不能被 $\mathfrak{p}$ 整除, 因为 $\mathfrak{q}$ 已经被假定是孤立的. 所以 $\mathfrak{q}$ 必定能被 $(\mathfrak{m},\mathfrak{p}^{\sigma})$ 整除:

$$\mathfrak{q}\equiv 0(\mathfrak{m},\mathfrak{p}^{\sigma}). \tag{15.17}$$

由 (15.16) 与 (15.17) 即得 (15.15).

推论 对于 $\sigma\geqslant\rho$, 有

$$\mathfrak{p}^{\sigma}\equiv 0(\mathfrak{q})\equiv 0(\mathfrak{m},\mathfrak{p}^{\sigma+1}),$$

从而

$$\mathfrak{p}^{\sigma}\equiv 0(\mathfrak{m},\mathfrak{p}^{\sigma+1}). \tag{15.18}$$

对于 $\sigma<\rho$ 来说, 关系 (15.18) 不再成立. 因为如果对于 $\sigma<\rho$,

$$\mathfrak{p}^{\sigma}\equiv 0(\mathfrak{m},\mathfrak{p}^{\sigma+1}).$$

那么通过乘以 $\mathfrak{p}^{\rho-\sigma-1}$ 将得到

$$\mathfrak{p}^{\rho-1}\equiv 0(\mathfrak{m}\mathfrak{p}^{\rho-\sigma-1},\mathfrak{p}^{\rho})\equiv 0(\mathfrak{m},\mathfrak{q})\equiv 0(\mathfrak{q}).$$

这与指数 ρ 的定义相违.

因此, *$\mathfrak{q}$的指数 ρ 是使得 (15.18) 成立的最小数.*

存在具有单位元的整环 $\mathfrak{o}$, 在其中 (因子链条件成立且) 每一个异于零理想的素理想都是极大的. 主理想环 (参看 3.8 节) 以及稍后将定义的数域或函数域内的某些“序模”都是这样的例子. 环 $\mathbb{Z}[\sqrt{-3}]$ 就是一个典型的例子. 这样的环的理想理论特别简单. 首先, 除零理想外一切准素理想都是单素的. 其次, 每两个互不相同且异于 (0) 的素理想都是无公因子的. 由此推出, 每两个属于互不相同且异于 (0) 的素理想的准素理想也是无公因子的. 最后, 一个理想的一切准素分支都是孤立的从而是唯一确定的. 于是, *每一个异于零的理想都可以唯一地被表示成无公因子的单素准素理想的交*. 根据 15.7 节, 这个交也等于积:

$$\mathfrak{a}=[\mathfrak{q}_1,\cdots,\mathfrak{q}_r]=\mathfrak{q}_1\cdots\mathfrak{q}_r.$$

在主理想环里, 这些准素理想 $\mathfrak{q}_i$ 都是素理想幂. 至于在一般环里是否也有这一情形, 则依赖于一个条件, 我们以后还要讨论, 就是“整闭性”条件.

15.9 商 环

在 3.3 节里, 我们已经对于每一个无零因子的交换环作出商域. 这种作法可以直接推移到有零因子的交换环上去, 只要在这个环里有非零因子 (即不是零因子的元素) 存在. 这时我们可以只取非零因子作为分母, 作一切商 a/b 的环, 这里 a 遍历一切环元素而 b 遍历一切非零因子.

我们还可以对分母更加以限制. 设在交换环 R 里, 一个由非零因子所成的非空集被给定, 它在含有每两个元素 s 与 t 的同时, 也含有它们的积 st. 于是商 a/s(a 取自 R, s 取自 S) 作成 R 的一个扩环: *商环*$R' = R/S$. 这个概念是 Grell 提出的 (*Math. Ann.*, 97: 449).

设 R' 是 R 的任意一个交换扩环, 那么 R 的每一理想 $\mathfrak{a}$ 在 R' 里生成一个理想 $\mathfrak{a}'$: $\mathfrak{a}$ 在 R' 内的*扩理想*. 反过来, R 与 R' 的一个理想 $\mathfrak{c}'$ 的交总是 R 的一个理想: $\mathfrak{c}'$ 在 R 内的*局限理想*. 局限理想 $\mathfrak{c}' \cap R$ 也叫做在 R 里的*特记理想*(相对于 R' 的).

关于扩理想与局限理想概念的一般研究可以在所提到的 Grell 的工作中找到. 在这里我们将只讨论商环的情形, 其中关系极为简单.

如果 $\mathfrak{a}$ 是 R 的一个理想, 那么在商环 R' 里扩理想 $\mathfrak{a}'$ 由一切商 a/s(a 属于 $\mathfrak{a}, s$ 属于 S) 所组成. 由这个 $\mathfrak{a}'$ 作局限理想 $\mathfrak{a}' \cap R$, 那么就恰好得到在 15.6 节里所定义的 S 分支 $\mathfrak{a}_S$, 就是一切这样的 x 的全体, 对于 S 里的一个 s, sx 属于 $\mathfrak{a}$.

反过来, 从商环 R' 的任意一个理想 $\mathfrak{a}'$ 出发而作局限理想

$$\mathfrak{a} = \mathfrak{a}' \cap R,$$

那么 $\mathfrak{a}$ 的扩理想仍是 $\mathfrak{a}'$. 这个扩理想与 R 的交就是 $\mathfrak{a}$, 从而在这时 $\mathfrak{a}_S = \mathfrak{a}$. 反过来, 如果 $\mathfrak{a}_S = \mathfrak{a}$, 那么 $\mathfrak{a}$ 是一个局限理想, 就是它的扩理想 $\mathfrak{a}'$ 的局限理想. 于是*在 R 里的特记理想 $\mathfrak{a}$ 由性质 $\mathfrak{a}_S = \mathfrak{a}$ 所刻画.*

由以上所述立刻推出, 在 R' 的理想 $\mathfrak{a}'$ 与 R 里的特记理想 $\mathfrak{a}$ 之间存在着如下的一个一对一的关系: $\mathfrak{a}$ 是 $\mathfrak{a}'$ 的局限理想而 $\mathfrak{a}'$ 是 $\mathfrak{a}$ 的扩理想. 因此交 $\mathfrak{a}' \cap \mathfrak{c}'$ 显然与交 $\mathfrak{a} \cap \mathfrak{c}$ 对应.

如果在 R 里对于理想的因子链条件成立, 那么这个条件特别对于特记理想成立, 从而也对于 R' 的理想成立. 在一个交表示

$$\mathfrak{a} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r] \tag{15.19}$$

里, 如此排列这些 $\mathfrak{q}_i$ 的次序使得只有 $\mathfrak{q}_{h+1}, \cdots, \mathfrak{q}_r$(或者属于它们素理想 $\mathfrak{p}_{h+1}, \cdots, \mathfrak{p}_r$) 含有 S 的元素, 那么经过扩张, 这些理想都变为 R' 的单位理想, 于是就像在 15.6

节里那样, 得到

$$\mathfrak{a}_S = [\mathfrak{q}_1, \cdots, \mathfrak{q}_h]. \tag{15.20}$$

在 (15.20) 式右端出现的 $\mathfrak{q}_i$ 具有性质 $\mathfrak{q}_S = \mathfrak{q}$. 从而是特记的. 同样 $\mathfrak{a}_S$ 也是特记的. 根据特记理想与它们的扩理想之间的一一对应, 我们由 (15.19) 得到对于扩理想的表示

$$\mathfrak{a}' = [\mathfrak{q}_1', \cdots, \mathfrak{q}_h']. \tag{15.21}$$

比较 (15.19) 与 (15.21), 我们看出, 从 R 过渡到 R' 时, 理想将会变少. 一切含有 S 的元素的理想的扩理想, 特别是准素理想 $\mathfrak{q}_{h+1}, \cdots, \mathfrak{q}^r$ 的扩理想都是单位理想. 只有特记理想 $\mathfrak{a}$(具有性质 $\mathfrak{a}_S = \mathfrak{a}$) 经过扩张后在这样的意义之下保持不受损失, 就是由 $\mathfrak{a}'$ 出发作局限理想 $\mathfrak{a}'$ 又可以返回来得到原来的理想 $\mathfrak{a} = \mathfrak{a}_S$.

习题 15.11 如果 $\mathfrak{q}$ 是准素理想而 $\mathfrak{p}$ 是属于它的素理想, 那么在商环 R' 里扩理想 $\mathfrak{q}'$ 也是准素的并且扩理想 $\mathfrak{p}'$ 是属于 $\mathfrak{q}'$ 的素理想.

习题 15.12 设在一个任意环 R' 里, $\mathfrak{q}'$ 是属于素理想 $\mathfrak{p}'$ 的一个准素理想, 那么在 R' 的任意子环 R 里, 局限理想 $\mathfrak{q} = \mathfrak{q}' \cap R$ 是准素的且属于素理想 $\mathfrak{p} = \mathfrak{p}' \cap R$.

广义商环

设 S 是 R 的一个乘法封闭集, 它含有零因子但是不含有零. 于是可以依照 Chevalley 的办法如此定义一个广义商环. 设 $\mathfrak{n} = (0)_S$ 是 R 里零理想的 S 分支. 我们首先作同余类环 $R^* = R/\mathfrak{n}$. S 的元素模 $\mathfrak{n}$ 的同余类作成 R^* 里的一个乘法封闭集 S^*, 它不再含有零因子. 于是可以作普通商环 $R' = R^*/S^*$. 这个环叫做由 R 与 S 所成的广义商环. 它的性质与普通商环类似. R 的一个理想 $\mathfrak{a}$ 的扩理想将被这样作出, 首先在同态 $R \to R'$ 之下得出 $\mathfrak{a}$ 的象 $\mathfrak{a}^*$, 然后作 $\mathfrak{a}^*$ 在 R' 里所生成的理想. 类似地, R' 的一个理想 $\mathfrak{c}'$ 的局限理想这样作出, 首先作 $\mathfrak{c}'$ 与 R^* 的交, 然后作这样元素的集, 它们模 $\mathfrak{n}$ 的同余类属于这个交.

至于进一步的讨论可以看 Northcott D G. *Ideal Theory.* Cambridge Tracts in Math., 42, §2.7.

15.10 一个理想一切幂的交

以下我们总是假定 $\mathfrak{o}$ 是一个有单位元的 Noether 环. 这个环叫做零准素的, 如果零理想是准素的, 换一句话, 如果由 $ab = 0$ 就有 $a = 0$ 或 $b^r = 0$.

Krull 在他的基本工作里①指出, 在一个零准素环 $\mathfrak{o}$ 里, 因而特别在一个整环

① Krull W. Primidealketten in allgemeinen Ringbereichen. S.-B. *Heidelberger Akad.,* 1928: 7, *Abh.*

里, 一个异于零的理想 $\mathfrak{a}$ 的一切幂的交是零理想. 对于一个素理想 $\mathfrak{p} \neq \mathfrak{o}$ 来说, 甚至于它的一切符号幂 $\mathfrak{p}^{(r)}$ 的交也是零理想. 由这些定理也可以得到关于任意环的结果. 这个研究的主要思想将在这里表现出来.

定理 1　设 $\mathfrak{a}$ 与 $\mathfrak{d}$ 是一个零准素环 $\mathfrak{o}$ 的理想, 且

$$\mathfrak{d} \subseteq \mathfrak{a}\mathfrak{d}, \tag{15.22}$$

那么或者 $\mathfrak{a} = \mathfrak{o}$ 或者 $\mathfrak{d} = (0)$.

证　设 $\mathfrak{d} = (d_1, \cdots, d_n)$. 于是由 (15.22) 得

$$d_i = \sum a_{ik} d_k. \tag{15.23}$$

像通常那样令 $\delta_{ik} = 0$, 对于 $i \neq k$ 且 $\delta_{ii} = 1$, 于是 (15.23) 也可以写成

$$\sum (\delta_{ik} - a_{ik}) d_k = 0. \tag{15.24}$$

这个线性方程组的行列式是

$$D = 1 - a,$$

这里 a 属于理想 $\mathfrak{a}$. 将方程 (15.24) 乘以行列式 D 的第 k 列的代数余子式, 并且相加, 我们得到

$$D d_k = 0,$$

从而对于理想 $\mathfrak{d}$ 的每一元素 d,

$$(1 - a) d = D d = 0.$$

由此推出：或者 $(1 - a)^r = 0$, 或者当 $1 - a$ 的任何幂都不等于零时, $d = 0$ 对于 $\mathfrak{d}$ 里的一切 d 成立. 在第一种情形我们有 $1 \equiv 0(\mathfrak{a})$, 从而 $\mathfrak{a} = \mathfrak{o}$. 在第二种情形将有 $\mathfrak{d} = (0)$.

定理 2　设 $\mathfrak{o}$ 是一个零准素环且 $\mathfrak{a} \neq \mathfrak{o}$, 那么 $\mathfrak{a}$ 的一切幂的交是零理想：

$$\mathfrak{d} = [\mathfrak{a}, \mathfrak{a}^2, \cdots] = (0). \tag{15.25}$$

证　首先应该证明 $\mathfrak{d} \subseteq \mathfrak{a}\mathfrak{d}$. 为此将 $\mathfrak{a}\mathfrak{d}$ 表示成准素理想的交：

$$\mathfrak{a}\mathfrak{d} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_r].$$

对于每一 $i, \mathfrak{a}\mathfrak{d}$ 能被 $\mathfrak{q}_i$ 整除, 因此或者 $\mathfrak{d}$ 或者某一幂 $\mathfrak{a}^n$ 能被 $\mathfrak{q}_i$ 整除. 然而 $\mathfrak{d}$ 可以被每一幂 $\mathfrak{a}^n$ 整除. 因此在两种情形都有 $\mathfrak{d} \subseteq \mathfrak{q}_i$. 这个关系对一切 i 成立, 所以

$$\mathfrak{d} = \mathfrak{a}\mathfrak{d}.$$

因此, 根据定理 1 得 $\mathfrak{d} = (0)$.

对于素理想 $\mathfrak{p} \neq \mathfrak{o}$ 来说, 还有较强的定理:

定理 3 在一个零准素环里, 一个异于 $\mathfrak{o}$ 的素理想 $\mathfrak{p}$ 的一切符号幂 $\mathfrak{p}^{(r)}$ 的交是零理想:

$$[\mathfrak{p}, \mathfrak{p}^{(2)}, \mathfrak{p}^{(3)}, \cdots] = (0). \tag{15.26}$$

证 设 S 是 $\mathfrak{o}$ 中不能被 $\mathfrak{p}$ 整除的元素的全体. 我们作商环 $\mathfrak{o}_S$. 令 $\mathfrak{p}$ 在 $\mathfrak{o}_S$ 内的扩理想是 $\mathfrak{P}$. $\mathfrak{p}^r$ 的扩理想显然是 $\mathfrak{P}^r$. 然而 $\mathfrak{P}^{r'}$ 的局限理想则是

$$(\mathfrak{p}^r)_S = \mathfrak{p}^{(r)}.$$

一切 $\mathfrak{p}^{(r)}$ 的交等于一切 $\mathfrak{P}^r$ 与 $\mathfrak{o}$ 的交. 根据定理 2, 一切 $\mathfrak{P}^r$ 的交是零理想. 因此一切 $\mathfrak{p}^{(r)}$ 的交是零理想.

定理 1 与定理 2 可以推广到在这里所考虑那样的任意环上去. 设 S 是一切元素 $s = 1 - a$ 的集, 此处 a 遍历理想 $\mathfrak{a}$. 集 S 是乘法封闭的, 从而可以定义零理想的 S 分支 $(0)_S$ 为这样 x 的集, 对于每一 x, 方程

$$(1-a)x = 0, \quad a\text{属于}\mathfrak{a}$$

成立. 现在有

定理 1a 若 $\mathfrak{d} \subseteq \mathfrak{a}\mathfrak{d}$, 则 $\mathfrak{d} \subseteq (0)_S$.

定理 2a $\mathfrak{a}$ 的一切幂的交是 $(0)_S$.

定理 1a 的证明直到方程

$$(1-a)d = 0$$

的得出都和定理 1 的证明完全一样.

由这个方程立刻推出

$$d \in (0)_S, \quad \text{对 } \mathfrak{d} \text{ 中的一切 } d.$$

定理 2a 的一半, 就是

$$[\mathfrak{a}, \mathfrak{a}^2, \cdots] \subseteq (0)_S,$$

可以同定理 2 完全一样来证明. 另一半

$$(0)_S \subseteq [\mathfrak{a}, \mathfrak{a}^2, \cdots]$$

是容易证明的. 设 x 属于 $(0)_S$, 那么

$$(1-a)x = 0,$$

从而 $x=ax$, 因此

$$x=ax=a^2x=a^3x=\cdots.$$

这样, x 可以被 a 的任意幂整除.

将定理 1 及定理 2 应用到关于一个准素理想 $\mathfrak{q}$ 的同余类环 $\mathfrak{o}/\mathfrak{q}$ 上, 于是得到

定理 1b　*若 $\mathfrak{q}$ 是一个准素理想而*

$$\mathfrak{d}\equiv 0(\mathfrak{a}\mathfrak{d},\mathfrak{q}), \tag{15.27}$$

那么或者 $(\mathfrak{a},\mathfrak{q})=\mathfrak{o}$ 或者 $\mathfrak{b}\equiv 0(\mathfrak{q})$.

定理 2b　*如果 $\mathfrak{o}$ 的一个元素 y 对于一切自然数 n 来说满足同余式*

$$y\equiv 0(\mathfrak{a}^n,\mathfrak{q}), \tag{15.28}$$

那么或者 $(\mathfrak{a},\mathfrak{q})=\mathfrak{o}$ 或者 $y\equiv 0(\mathfrak{q})$.

习题 15.13　在一个有单位元的 Noether 环 $\mathfrak{o}$ 里, 一个素理想 $\mathfrak{p}\neq\mathfrak{o}$ 的一切符号幂的交等于 $(0)_s$.

习题 15.14　当取一个任意理想 $\mathfrak{m}$ 来代替准素理想 $\mathfrak{q}$ 时, 定理 1b 与 2b 应该怎样表述 (将定理 1a 与 2a 应用到同余类环 $\mathfrak{o}/\mathfrak{m}$ 上)?

15.11　理想的长度, Noether 环中的素理想链

定理 1 及定理 2(15.10 节) 以及它们的变形在上述的 Krull 的工作里同时被用来导出关于素理想链

$$\mathfrak{p}_1\supset\mathfrak{p}_2\supset\cdots$$

中断的定理. 在表述这个定理之前, 我们首先需要说明关于一个准素理想的长度的概念.

设 $\mathfrak{q}$ 是在一个 Noether 环 $\mathfrak{o}$ 中属于素理想 $\mathfrak{p}$ 的一个准素理想. 属于同一素理想 $\mathfrak{p}$, 末项为 $\mathfrak{q}$ 的一个准素理想序列:

$$\mathfrak{q}_1\supset\mathfrak{q}_2\supset\cdots\supset\mathfrak{q}_l=\mathfrak{q}$$

叫做*关于准素理想 $\mathfrak{q}$ 的一个真正规列*. 这个“真”字需要加以说明, 就是每一个后面的理想都是前一个的真倍理想的意思. 数 l 叫做这个正规列的*长度*. 如果这个序列不能再通过插入另外一些准素理想而被加细时, 那么就称这个序列为*关于准素理想 $\mathfrak{q}$ 的一个合成列*.

我们要证明, 每个关于准素理想 $\mathfrak{q}$ 的真正规列可以加细成为一个合成列, 并且所有合成列具有相同的长度. 这个长度称为*准素理想 $\mathfrak{q}$ 的长度*.

在证明时, 我们可以只限于 $\mathfrak{q}$ 是零理想的情形. 一般情形可以通过对 $\mathfrak{q}$ 作同余类环而归到这一情形. 在这个同余类环里, 一切准素理想都是零理想 $\mathfrak{q}$ 的因子, 从而一切素理想都是 $\mathfrak{p}$ 的因子.

令 S 是 $\mathfrak{o}$ 中一切不能被 $\mathfrak{p}$ 整除的元素的集, 通过向商环 $\mathfrak{o}' = \mathfrak{o}/S$ 过渡, 这时情况将更为简单. 在由 $\mathfrak{o}$ 向 $\mathfrak{o}'$ 的扩张之下, $\mathfrak{p}$ 的一切真因子生成单位理想 $\mathfrak{o}'$, 只有 $\mathfrak{p}$ 生成一个异于 $\mathfrak{o}'$ 的素理想 $\mathfrak{p}'$. 因为 $\mathfrak{o}'$ 的每一个素理想都是 $\mathfrak{o}$ 的一个素理想 (就是它的局限理想) 的扩理想, 因此, 在 $\mathfrak{o}'$ 里除 $\mathfrak{o}'$ 本身之外只存在唯一的一个素理想 $\mathfrak{p}'$. 因此在一个理想 $\mathfrak{m}' \neq \mathfrak{o}'$ 的交表示里只能有唯一的准素理想 (属于素理想 $\mathfrak{p}'$) 出现, 这就是说:

在 $\mathfrak{o}'$ 里, 除 $\mathfrak{o}'$ 本身外, 每一个理想都是属于素理想 $\mathfrak{p}'$ 的准素理想.

从现在起可以将 $\mathfrak{o}'$ 与 $\mathfrak{p}'$ 仍旧叫做 $\mathfrak{o}$ 与 $\mathfrak{p}$. 我们把 $\mathfrak{o}$ 看成以 $\mathfrak{o}$ 本身为算子集的带算子的群. 可许子群就是 $\mathfrak{o}$ 的理想, 即 $\mathfrak{o}$ 本身以及属于素理想 $\mathfrak{p}$ 的准素理想. 在群论意义下一个真正规群列

$$\mathfrak{o} \supset \mathfrak{q}_1 \supset \mathfrak{q}_2 \supset \cdots \supset \mathfrak{q}_l = (0),$$

当略去首项 $\mathfrak{o}$ 时, 就给出一个关于理想 $\mathfrak{q}_l = (0)$ 的真正规列.

在第 6 章里已经证明: 如果在一个带算子群里存在一个合成列, 那么每一个真正规群列都可以加细到一个合成列, 并且一切合成列都具有相同的长度 l. 因此只要证明, 在 $\mathfrak{o}$ 里合成列存在.

为了这个目的, 我们作正规列

$$\mathfrak{p} \supset \mathfrak{p}^2 \supset \cdots \supset \mathfrak{p}^\rho = (0).$$

我们可以把 $\mathfrak{p}^k/\mathfrak{p}^{k+1}$ 看成以 $\mathfrak{o}/\mathfrak{p}$ 为算子集的向量空间. 因为 $\mathfrak{p}$ 是极大的, 所以 $\mathfrak{o}/\mathfrak{p}$ 是一个域. 由于 $\mathfrak{p}^k$ 有一个有限理想基, 所以这个向量空间是有限维的. 因此存在一个从 $\mathfrak{p}^k$ 到 $\mathfrak{p}^{k+1}$ 的有限合成列. 我们把这些合成列对于 $k = 1, 2, \cdots, \rho - 1$ 依次排列, 就得到一个从 $\mathfrak{p}$ 到 (0) 的合成列, 于是定理完全被证明.

Krull 关于准素理想链的定理完全基于以下的定理.

主理想定理 *设 $(b) \neq \mathfrak{o}$ 是一个主理想又 $\mathfrak{p}$ 是一个属于 (b) 的孤立素理想, 那么每一个真素理想链*

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \cdots$$

在 $\mathfrak{p}_1$ 已经终止.

证 假定存在一个链

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_2. \tag{15.29}$$

通过作 mod $\mathfrak{p}_2$ 的同余类可以使 $\mathfrak{p}_2$ 变成零理想. 由此将推出, 这个环没有零因子. 现在向商环 $\mathfrak{o}/S$ 过渡, 此处 S 是 $\mathfrak{o}$ 中不能被 $\mathfrak{p}$ 整除的元素的集, 于是一切不能被 $\mathfrak{p}$ 整除的理想变为单位理想, 而链 (15.29) 里被 $\mathfrak{p}$ 整除的理想仍旧不相同, 并且是素的. 这个商环, 仍记作 $\mathfrak{o}$, 有单位元并且没有零因子. 因为一切属于 (b) 的素理想除 $\mathfrak{p}$ 以外都变为单位理想, 所以 (b) 现在变成一个属于素理想 $\mathfrak{p}$ 的准素理想. 同样, (b) 的一切因子除 $\mathfrak{o}$ 以外现在是属于素理想 $\mathfrak{p}$ 的准素理想. 通过向商环过渡, $\mathfrak{o}$ 的理想理论将大为简化, 使得以下的证明非常容易.

我们仍旧以 $\mathfrak{p}_1^{(r)}$ 表示 $\mathfrak{p}_1$ 的 r 次符号幂. 链

$$(\mathfrak{p}_1^{(1)}, b) \supseteq (\mathfrak{p}_1^{(2)}, b) \supseteq \cdots$$

里的理想都是 b 的因子, 从而根据上面的讨论, 它们都是属于素理想 $\mathfrak{p}$ 的准素理想. 在这个链里不相同的理想的个数不能大于准素理想 (b) 的长度, 因此从某一固定的位置起, 这个链的一切理想都相等：

$$(\mathfrak{p}_1^{(s)}, b) = (\mathfrak{p}_1^{(s+1)}, b) = \cdots .$$

现在设 $m \geqslant s$. 我们首先证明

$$\mathfrak{p}_1^{(m)} \subseteq (b\mathfrak{p}_1^{(m)}, \mathfrak{p}_1^{(m+1)}). \tag{15.30}$$

令 x 是 $\mathfrak{p}_1^{(m)}$ 的一个元素. 于是有

$$x \in (\mathfrak{p}_1^{(m)}, b) = (\mathfrak{p}_1^{(m+1)}, b),$$

因此

$$x = y + br, \quad y \in \mathfrak{p}_1^{(m+1)},$$

从而

$$br = x - y \equiv 0(\mathfrak{p}_1^{(m)}).$$

现在根据定义, $\mathfrak{p}_1^{(m)}$ 是准素的且 b 不能被属于 $\mathfrak{p}_1^{(m)}$ 的素理想 $\mathfrak{p}_1$ 整除, 因此 r 必定能被 $\mathfrak{p}_1^{(m)}$ 整除. 由此得

$$x = y + br \equiv 0(\mathfrak{p}_1^{(m+1)}, b\mathfrak{p}_1^{(m)}),$$

从而 (15.30) 被证明.

根据定理 1b (15.10 节), 由 (15.30) 推出

$$\mathfrak{p}_1^{(m)} \subseteq \mathfrak{p}_1^{(m+1)},$$

于是 $\mathfrak{p}_1^{(m)} = \mathfrak{p}_1^{(m+1)}$ 对于一切 $m \geqslant s$ 成立, 这就是说,

$$\mathfrak{p}_1^{(s)} = \mathfrak{p}_1^{(s+1)} = \mathfrak{p}_1^{(s+2)} = \cdots . \tag{15.31}$$

环 $\mathfrak{o}$ 没有零因子. 于是根据定理 3(15.10 节), $\mathfrak{p}_1$ 的符号幂的交是零理想. 因此由 (15.31) 得

$$\mathfrak{p}_1^{(s)} = (0). \tag{15.32}$$

然而 $\mathfrak{p}_1^{(s)}$ 是属于素理想 $\mathfrak{p}_1$ 的一个准素理想, 而 (0) 是素理想 $\mathfrak{p}_2$. 这就导致矛盾. 因此不可能有形如 (15.29) 的链.

反复应用这个主理想定理, Krull 证明了以下的推广：

若 $\mathfrak{p}$ 是一个属于 $\mathfrak{m} = (b_1, \cdots, b_r)$ 的孤立素理想且 $\mathfrak{m} \neq \mathfrak{o}$, 那么每一个真素理想链

$$\mathfrak{p} \supset \mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \cdots \tag{15.33}$$

最迟在 $\mathfrak{p}_r$ 处终止.

这个定理特别当

$$\mathfrak{m} = \mathfrak{q} = (b_1, \cdots, b_r)$$

是一个准素理想而 $\mathfrak{p}$ 是属于它的素理想时成立. 因为每一个理想都具有一个有限基, 于是得到

定理 *每一个真素理想链 (15.33) 在有限步后必定终止.*

关于这个结果的证明以及它对于局部环理论的应用可以在 Northcott. *Ideal Theory* 一书中找到.

第 16 章 多项式理想论

在这一章里, 我们将把一般理想论应用到多项式环 $\mathfrak{o} = K[x_1, \cdots, x_n]$ 上, 这里 K 是一个任意域. 除一般理想论以外, 只假定第 1 章 ~6 章以及第 10 章是已知的.

16.1 代数流形

设 Ω 是基域 K 的一个任意扩域. Ω 的一个 n 元序列 $\xi_1, \cdots, \xi_n$ 叫做仿射空间 $A_n(\Omega)$的一个点 ξ. 点 ξ 叫做 $\mathfrak{o} = K[x_1, \cdots, x_n]$ 的多项式 f 的一个零点, 如果 $f(\xi_1, \cdots, \xi_n) = 0$.

所谓 $A_n(\Omega)$ 内的一个代数流形 M, 或者简称流形 M, 指的是有限个多项式 $f_1, \cdots, f_r$ 的公共零点的集, 因而也就是方程

$$f_1(\xi) = 0, \cdots, f_r(\xi) = 0$$

的一切解的集.

由多项式 $f_1, \cdots, f_r$ 作理想 $\mathfrak{a} = (f_1, \cdots, f_r)$, 我们看到, $f_1, \cdots, f_r$ 的一切公共零点是理想 $\mathfrak{a}$ 的一切多项式

$$f = g_1 f_1 + \cdots + g_r f_r$$

的零点, 因此 M 也可以看成这个理想的一切多项式的公共零点的集, 或者也说, 是理想$\mathfrak{a}$的零点的集. 根据 Hilbert 基定理 (15.1 节), $\mathfrak{a}$ 具有一个有限基, 因此, 一个代数流形 M 由 $\mathfrak{o} = K[x_1, \cdots, x_n]$ 的一个理想 $\mathfrak{a}$ 在 $A_n(\Omega)$ 内的零点所组成, 我们称 M 为理想 $\mathfrak{a}$ (或理想 $\mathfrak{a}$ 的零点)的流形.

$\mathfrak{a}$ 的一个因子, 即一个含 $\mathfrak{a}$ 的理想 $\mathfrak{c}$ 确定 M 的一个子流形. 然而也有可能不同的理想确定同一个流形 M. 在一切这样的理想中有一个特殊的理想, 就是在 M 的所有点取值零的一切 多项式的集. 这个集自然是一个理想 $\mathfrak{m}$. 称 $\mathfrak{m}$ 为属于 M 的理想. $\mathfrak{m}$ 的流形仍是 M, 因此 M 由 $\mathfrak{m}$ 唯一确定 (反过来 $\mathfrak{m}$ 也由 M 唯一确定).

在环 $\mathfrak{o} = K[x_1, \cdots, x_n]$ 里, 因子链条件成立, 因而极大条件也成立 (15.1 节). 由此得出

对于流形的极小原理 *在每一个由流形 M 所成的非空集中, 存在一个极小流形 M^*, 就是这样的一个流形, 它不包含这个集的其他的流形.*

证 每一个流形 M 都有一个属于它的理想 $\mathfrak{m}$, 并且对于不同的流形 M, 属于它们的理想 $\mathfrak{m}$ 也不同. 在这些理想 $\mathfrak{m}$ 的集里存在一个极大理想 $\mathfrak{m}^*$, 它属于一个流形 M^*. 这个 M^* 就是这个集内的一个极小流形.

如果一个多项式 f 在一个流形 M 的一切点处都取值零, 那么就说, f 包含 M (因为这时 $f=0$ 的流形包含流形 M). 于是属于 M 的理想 $\mathfrak{m}$ 由一切包含 M 的多项式所组成.

两个流形 M 与 N 的交 $M\cap N$ 仍是一个流形. 如果 M 由 $\mathfrak{a}=(f_1,\cdots,f_r)$ 的零点所组成而 N 由 $\mathfrak{b}=(g_1,\cdots,g_s)$ 的零点所组成, 那么 $M\cap N$ 由理想

$$(\mathfrak{a},\ \mathfrak{b})=(f_1,\cdots,f_r,\ g_1,\cdots,g_s)$$

的零点所组成.

并 $M\cup N$ 也是一个流形. 它是由交 $\mathfrak{a}\cap\mathfrak{b}$(或者也由积 $\mathfrak{a}\cdot\mathfrak{b}$) 所确定的. 首先, 这个并里的每一点或者是 $\mathfrak{a}$ 的一切多项式的零点, 或者是 $\mathfrak{b}$ 的一切多项式的零点, 从而在每一种情形都是 $\mathfrak{a}\cap\mathfrak{b}$ 的一切多项式的零点 (特别是 $\mathfrak{a}\cdot\mathfrak{b}$ 的一切多项式的零点). 然而, 若一个点 ξ 不属于并 $M\cup N$, 那么在 $\mathfrak{a}$ 里有一个多项式 f, 同时在 $\mathfrak{b}$ 里有一个多项式 g, 它们在点 ξ 的值不为零. 这时属于 $\mathfrak{a}\cap\mathfrak{b}$(或 $\mathfrak{a}\cdot\mathfrak{b}$) 的多项式 fg 在点 ξ 的值不为零, 从而 ξ 不是 $\mathfrak{a}\cap\mathfrak{b}$(或 $\mathfrak{a}\cdot\mathfrak{b}$) 的零点. 因此 $\mathfrak{a}\cap\mathfrak{b}$(同时 $\mathfrak{a}\cdot\mathfrak{b}$) 的零点是 $M\cup N$ 的点并且只能是 $M\cup N$ 的点.

正如在代数几何里通常所作的那样, 从现在起我们将只限于考虑非空的流形.

如果一个流形 M 能表示成两个 (非空) 真子流形的并, 那么就称它为*复合的*或*可约的*. 如果这两个子流形可以通过系数取自同一基域 K 的方程来定义, 那么就说, M*在基域 K 上是可约的*. 一个非可约流形叫做*不可约的* 或*不可分解的* (在基域 K 上).

判定标准 *一个流形 M 在 K 上不可约, 当且仅当属于 M 的理想是一个素理想, 即由“fg包含M”可得 f 或 g 包含M.*

证 首先设 M 可约: $M=M_1\cup M_2$, 此处 M_1 与 M_2 都是 M 的真子流形. 在属于 M_1 的理想中存在一个多项式 f, 它不包含 M, 否则将有 $M_1\supseteq M$. 同理, 在属于 M_2 的理想中存在一个多项式 g, 它也不包含 M. 积 fg 包含 M_1 及 M_2, 因而包含 M. 因此属于 M 的理想是非素的.

其次设 M 不可约. 现在, 如果, fg 是一个积, 它包含 M 而 f 与 g 都不包含 M, 那么可以把 M 表示成两个真子流形 M_1 或 M_2 的并, 它们可以如下定义: M_1 是由 M 的一切满足方程 $f=0$ 的点所组成的而 M_2 是由 M 的一切满足方程 $g=0$ 的点所组成的. 于是 M 的每一点 ξ 或者属于 M_1 或者属于 M_2, 因为由 $f(\xi)g(\xi)=0$ 就有 $f(\xi)=0$ 或 $g(\xi)=0$. 然而这与 M 不可约的假设相违.

于是我们证明了:

如果一个不可约流形 M 被包含在两个流形 M_1 与 M_2 的并里, 那么 M 或者被包含在 M_1 里或者被包含在 M_2 里.

当 M 被包含在 $M_1, \cdots, M_r$ 的并里时, 相应的论断也成立.

分解定理 每一个在 K 上定义的流形 M 都可以表示成有限个在 K 上不可约流形的并.

证 假设存在着某些流形 M, 它们都不能表示成不可约流形的并, 那么在这样的流形 M 的集中, 存在一个极小流形 M^*. 这个流形一定是可约的, 因而可以表示成两个真子流形 M_1 与 M_2 的并. 由于 M^* 的极小性, M_1 与 M_2 都可以表示成不可约流形的并, 从而 M^* 也可以表成不可约流形的并, 这与假设矛盾. 这就证明了分解定理.

我们可以从分解

$$M = I_1 \cup I_2 \cup \cdots \cup I_r \tag{16.1}$$

中去掉多余的项, 于是这个分解除次序外是唯一的. 事实上, 如果

$$M = J_1 \cup J_2 \cup \cdots \cup J_s \tag{16.2}$$

是另一个分解, 那么 I_1 含在这些 J_i 的并里, 从而含在某一 J_i 里, 于是对 J 适当编号, 可以设 I_1 包含在 J_1 里. 同样, J_1 包含在某一 I_k 里:

$$I_1 \subseteq J_1 \subseteq I_k.$$

如果 $k \neq 1$, 那么 I_1 在 (16.1) 里是多余的. 因此 $k = 1$ 而 $I_1 = J_1$. 完全同样, 我们得到 $I_2 = J_2, \cdots, I_r = J_r$ 且 $r = s$, 于是分解的唯一性被证明.

如果只考虑属于仿射空间 $A_n(\Omega)$ 的一个固定子集的点, 同样的定理也成立①.

16.2 泛 域

在古典的代数几何里, 点 ξ 的坐标所取值的域 Ω 总是复数域. 然而, 在新的代数几何里, 也可以从一个任意基域 K 出发. 点 ξ 的坐标所取值的域 Ω, 按照 Weil 的作法, 取做 K 上的*泛域* 是适当的, 这就是说, 首先假定 Ω 是代数封闭的, 其次又假定 Ω 在 K 上有无限超越次数. 如果 K 已被给定, 那么就可以作出一个这样的泛域, 我们首先在 K 上添加无限多个不定元 $u_1, u_2, \cdots$, 然后再依 10.1 节作代数封闭.

① 参看 Habicht W. Topologische eigenschaften algebraisher mannigfaltigkeiten. *Math. Ann.*, 122: 181.

关于一个在 K 上不可约流形当基域扩张时的分解, 请看作者本人的工作 Über A. Weils Neubegründung der algebr. geom.. *Abh. Math. Sem., Hamburg*, 22: 158.

泛域的作用基于以下定理:

定理　通过添加有限多个域元素 $\alpha_1,\cdots,\alpha_n$ 到 K 上而得到的每一扩域 $K(\alpha_1,\cdots,\alpha_n)$ 都可以同构地嵌入 Ω. 换一句话说, 如果在 K 的任一扩域 Λ 内的任意 n 个元素 $\alpha_1,\cdots,\alpha_n$ 被给定, 那么存在一个使 K 的元素不动且将 $\alpha_1,\cdots,\alpha_n$ 变到 Ω 的元素 $\alpha'_1,\cdots\alpha'_n$ 的同构

$$K(\alpha_1,\cdots,\alpha_n)\cong K(\alpha'_1,\cdots,\alpha'_n).$$

证　我们可以将 $\alpha_1,\cdots,\alpha_n$ 如此编号, 使得 $\alpha_1,\cdots,\alpha_r$ 在 K 上代数无关而其余的 α_i 在 $K(\alpha_1,\cdots,\alpha_r)$ 上是代数的. 现在我们在 Ω 里选取 $\alpha'_1,\cdots,\alpha'_r$ 在 K 上代数无关. 于是存在一个同构

$$K(\alpha_1,\cdots,\alpha_r)\cong K(\alpha'_1,\cdots,\alpha'_r), \tag{16.3}$$

它使 K 的元素不动并且将 $\alpha_1,\cdots,\alpha_r$ 变到 $\alpha'_1,\cdots,\alpha'_r$. 如果 $r=n$, 那么我们已经证完. 如果 $r<n$, 设 α_{r+1} 是一个系数在 $K(\alpha_1,\cdots,\alpha_r)$ 内的不可约多项式 $\varphi(x)$ 的一个零点. 于是有一个系数在 $K(\alpha'_1,\cdots,\alpha'_r)$ 内的不可约多项式 $\varphi'(x)$ 与它对应, 这个多项式在 Ω 内有一个零点 α'_{r+1}. 根据 18.1 节, 可以将同构 (16.3) 开拓成一个同构

$$K(\alpha_1,\cdots,\alpha_r,\alpha_{r+1})\cong K(\alpha'_1,\cdots,\alpha'_r,\alpha'_{r+1}), \tag{16.4}$$

在这个同构之下 α_{r+1} 变到 α'_{r+1}. 如此继续下去, 最后就得出所求的同构

$$K(\alpha_1,\cdots,\alpha_n)\cong K(\alpha'_1,\cdots,\alpha'_n). \tag{16.5}$$

16.3　素理想的零点

仍设 Ω 是基域 K 上的一个泛域, 又设 $\mathfrak{o}$ 是多项式环 $K[x_1,\cdots,x_n]$. 如果 $\xi_1,\cdots,\xi_n$ 是 K 的任一扩域的元素, 那么根据 16.2 节, 我们总可以用一个域同构将 $\xi_1,\cdots,\xi_n$ 变为 Ω 里的元素. 于是对于下面的定理来说, 不论是把 $\xi_1,\cdots,\xi_n$ 看成 Ω 的元素, 还是看成 K 的任一扩域 Λ 的元素都是等价的. 我们取 ξ_i 作为 Ω 的元素, 于是 ξ 是仿射空间 $A_n(\Omega)$ 的一个点.

这样的一个点 ξ 叫做一个理想 $\mathfrak{p}$ 的一般零点, 如果由 $f\in\mathfrak{p}$ 就有 $f(\xi)=0$, 并且反过来也成立. 这样一来, 理想 $\mathfrak{p}$ 恰由具有性质 $f(\xi)=0$ 的多项式 $f(x)$ 组成. 我们立刻就会看到, 这样的一个理想必定是素的. 我们将进一步指出, 每一个点 ξ 都是一个唯一确定的素理想 $\mathfrak{p}\neq\mathfrak{o}$ 的一般零点, 并且反过来, 每一个素理想 $\mathfrak{p}\neq\mathfrak{o}$ 除同构外都具有一个唯一确定的一般零点 ξ.

定理 1　设 $\xi_1, \cdots, \xi_n$ 是 K 的一个任意扩域的元素, 那么 $\mathfrak{o} = K[x_1, \cdots, x_n]$ 中满足 $f(\xi) = 0$ 的多项式 f 在 $\mathfrak{o}$ 中作成一个异于 $\mathfrak{o}$ 的素理想.

证　由 $f(\xi) = 0$ 与 $g(\xi) = 0$ 得 $f(\xi) - g(\xi) = 0$. 由 $f(\xi) = 0$ 得 $f(\xi)h(\xi) = 0$. 于是所考虑的多项式作成一个理想.

由 $f(\xi)g(\xi) = 0$ 及 $g(\xi) \neq 0$ 得 $f(\xi) = 0$, 因为域没有零因子. 于是这个理想是素的. 因为这个理想不含单位元, 所以它异于 $\mathfrak{o}$.

例　设 $\xi_1, \cdots, \xi_n$ 是系数在域 K 内一个不定元 t 的线性函数

$$\xi_i = \alpha_i + \beta_i t. \tag{16.6}$$

于是, 所说的素理想由一切具有以下性质的多项式 $f(x_1, \cdots, x_n)$ 组成, 对于这样的多项式来说, $f(\alpha_1 + \beta_1 t, \cdots, \alpha_n + \beta_n t)$ 关于 t 恒等于零, 或者说 (几何的表述) 是由一切这样的多项式所组成, 它们在由参数表示式 (16.6) 在 n 维空间所定义的直线的一切点处等于零. 这个例子可以用来说明这一节以及下一节的一切定理.

定理 2　如果将 $\mathfrak{p}$ 理解为在定理 1 所作的素理想, 那么$\varLambda = K(\xi_1, \cdots, \xi_n)$与 $\mathfrak{o}$ 对$\mathfrak{p}$的同余类域 Π 同构, 并且还可以使元素 $\xi_1, \cdots, \xi_n$ 与 $x_1, \cdots, x_n$ 的同余类对应.

证　设 $\mathfrak{L}$ 是 $\varLambda$ 中可以写成 $\xi_1, \cdots, \xi_n$ 的多项式的那些元素所成的环. $\varLambda = K(\xi_1, \cdots, \xi_n)$ 是 $\mathfrak{L}$ 的商域. 对于 $\mathfrak{L}$ 的每一元素 $f(\xi_1, \cdots, \xi_n)$, 令同余类环 $\mathfrak{o}/\mathfrak{p}$ 中由 $f(x_1, \cdots, x_n)$ 所代表的元素与它对应. 因为由 $f(\xi) - g(\xi) = 0$ 就有 $f - g \equiv 0(\mathfrak{p})$ 或 $f \equiv g(\mathfrak{p})$, 反过来也对, 所以这个对应是一对一的. 至于和与积对应着和与积, 是显然的. 于是环 $\mathfrak{L}$ 与 $\mathfrak{o}/\mathfrak{p}$ 同构. 因此, 商域 $\varLambda$ 与 Π 也必须同构.

定理 1 是说, 每一点 ξ 都是一个唯一的素理想 $\mathfrak{p}$ 的零点. 定理 2 是说, 如果不计同构, 点 ξ 由 $\mathfrak{p}$ 唯一确定. 我们现在证明

定理 3　每一个异于 $\mathfrak{o}$ 的素理想在泛域 $\varOmega$ 内有一个一般零点.

证　对于 $\mathfrak{o}$ 的多项式, 令一个新的集 $\mathfrak{o}'$ 的元素与它们对应, 这个集包含系数域 K, 并且对于两个对 $\mathfrak{p}$ 同余的多项式, 有相同的元素与它们对应, 而不同余的多项式有不同的元素与它们对应. 这总是可能的, 因为由于 $\mathfrak{p} \neq \mathfrak{o}$, K 中两个元素对 $\mathfrak{p}$ 同余当且仅当它们相等. 我们把对应于元素 $x_1, \cdots, x_n$ 的元素记作 $\xi_1, \cdots, \xi_n$.

集 $\mathfrak{o}'$ 被一对一地映到 $\mathfrak{o}$ 对 $\mathfrak{p}$ 的同余类环上. 于是, 如果在 $\mathfrak{o}'$ 中定义一个加法和一个乘法, 使得这个加法与乘法分别对应于同余类环的加法与乘法, 那么 $\mathfrak{o}'$ 与同余类环同构, 因而 $\mathfrak{o}'$ 没有零因子并且可以作商域 $\varLambda$.

$\mathfrak{o}'$ 的每一元素至少与 $\mathfrak{o}$ 的一个多项式 f 对应, 从而可以写作 $f(\xi_1, \cdots, \xi_n)$. 于是 $\mathfrak{o}' = K[\xi_1, \cdots, \xi_n]$ 且 $\varLambda = K(\xi_1, \cdots, \xi_n)$. 根据 16.2 节, $\varLambda$ 可以同构地嵌入泛域 $\varOmega$ 内. 因此可以认为 $\varLambda \subseteq \varOmega$. 元素 $f(\xi_1, \cdots, \xi_n)$ 等于零, 当且仅当多项式 f 属于零类 $\bmod \mathfrak{p}$. 于是 ξ 是 $\mathfrak{p}$ 的一个一般零点, 定理 3 被证明.

根据定理 3, 每一素理想 $\mathfrak{p} \neq \mathfrak{o}$ 在泛域 Ω 内有一个一般零点 ξ, 由定理 2, 这个点如果不计同构是由 $\mathfrak{p}$ 唯一确定的. 点 ξ 是 $\mathfrak{p}$ 的一个零点, 因而在 $\mathfrak{p}$ 的零点流形 M 内. 属于 M 的素理想仍是 $\mathfrak{p}$. 因为如果一个多项式 f 在 M 的一切点处都等于零, 那么特别有 $f(\xi) = 0$ 从而 $f \in \mathfrak{p}$. 因为属于 M 的理想是素的, 所以 M 不可约. 于是有

定理 4　*每一个素理想 $\mathfrak{p} \neq \mathfrak{o}$ 有一个由它的零点所组成的不可约流形, 并且 $\mathfrak{p}$ 就是属于这个流形的理想.*

我们从一个不可约流形 M 出发, 于是根据 16.1 节, 属于 M 的理想 $\mathfrak{p}$ 是素的. $\mathfrak{p}$ 的零点恰好就是 M 的点. 如果 ξ 是 $\mathfrak{p}$ 的一个一般零点, 那么就称 ξ 为 M 在K上的一个一般点. 回到定义上, 这就是说:

M的一个点 ξ 叫做 M 在K上的一个一般点, 如果每一个系数在K中被 ξ 所满足的方程 $f(\xi) = 0$ 同时被 M 的一切点所满足.

根据定理 3, 每一个不可约流形都有一个一般点. 反过来, 如果一个流形 M 有一个一般点 ξ, 那么根据定理 1, 属于 M 的理想是素的, 从而 M 不可约. 于是有

定理 5　*当且仅当 M 在 K 上不可约时, M 有一个在 K 上的一般点.*

习题 16.1　$K[x_1, x_2, x_3]$ 的理想

$$(x_1x_3 - x_2^2, x_2x_3 - x_1^3, x_3^2 - x_1^2x_2)$$

是素的, 因为它有一般零点 (t^3, t^4, t^5).

16.4　维　　数

设 ξ 是一个不可约流形 M 在 K 上的一个一般点, 也就是属于 M 的素理想 $\mathfrak{p}$ 的一个一般零点. 如果 r 是 $\{\xi_1, \cdots, \xi_n\}$ 的超越次数, 那么在这些 ξ_i 里恰有 r 个代数无关的, 例如 $\xi_1, \cdots, \xi_r$, 而其余的都与这 r 个代数相关. 我们可以选取 $\xi_1, \cdots, \xi_r$ 作为不定元 $t_1, \cdots, t_r$. 于是一切 ξ_i 都是这 r 个不定元的代数函数. 当一般点通过一个域同构变为另一个一般点 ξ' 时, 超越次数 r 保持不变. 因此 r 只依赖于 $\mathfrak{p}$, 并且叫做素理想 $\mathfrak{p}$ 或流形 M 的维数.

素理想 $\mathfrak{p} \neq \mathfrak{o}$ 的维数自然在 0 与 n 之间. 对于单位理想 $\mathfrak{o}$, 它没有零点, 我们约定维数为 -1.

如果 ξ 是一个素理想 $\mathfrak{p}$ 的一个一般零点, ξ' 是同一理想的一个任意零点, 那么对于 $K[\xi]$ 的每一多项式 $f(\xi)$, 令 $K[\xi']$ 的一个多项式 $f(\xi')$ 与它对应. 因为由 $f(\xi) = g(\xi)$ 就有 $f(x) \equiv g(x)(\mathfrak{p})$, 从而 $f(\xi') = g(\xi')$, 所以对应 $f(\xi) \to f(\xi')$ 是单值的. 因为这个对应显然将和变成和, 积变成积, 所以是一个同态:

$$K[\xi] \sim K[\xi']. \tag{16.7}$$

如果这个对应是同构, 那么自然 ξ' 也是 $\mathfrak{p}$ 的一个一般零点, 反过来也对.

对于一个零维理想 $\mathfrak{p}$ 来说, 一切 ξ 在 K 上都是代数的. 从而 ξ 的一切有理函数已经是有理整函数：$K(\xi)=K[\xi]$. 因此 $K[\xi]$ 是一个域. 这时如果 ξ' 仍是一个任意零点, 那么同态 (16.7) 必定是一个同构. 因为一个域除一一同态及将整个域映成零环的同态以外没有其他的同态. 于是以下定理成立：

定理　*一个零维素理想的一切零点都是一般零点并且彼此等价*[①].

在这一情形, 坐标 $\xi_1,\cdots,\xi_n$ 或 $\xi'_1,\cdots,\xi'_n$ 是 K 上的代数元. 如果将零点 ξ 或 ξ' 限制在一个固定的泛域内, 那么一切这样的零点都在 K 上共轭. 这些在 Ω 内共轭点的个数最多等于 (并且当 $K(\xi)$ 是可分的时候, 恰好等于)$K(\xi)$ 在 K 上的域次数. 于是

一个零维不可约流形由有限多个在K上共轭的点组成.

特别当域 K 已经是代数封闭的时候, 在域 K 内只有一个零点 ξ, 而所属的理想是

$$\mathfrak{p}=(x_1-\xi_1,\cdots,x_n-\xi_n).$$

定理　*一个 r 维素理想的不同零点具有超越次数 $\leqslant r$, 并且当一个零点的超越次数恰好等于 r 时, 这个零点是一般零点.*

证　设 ξ' 是一个具有超越次数 s 的零点, 那么同态 (16.7) 存在. 设 $\xi'_1,\cdots,\xi'_s$ 代数无关, 那么 $\xi_1,\cdots,\xi_s$ 也代数无关. 因为 ξ 间的每一代数关系将转移为 ξ' 间的同一代数关系. 因此 $r\geqslant s$. 如果 $r=s$, 那么一切 ξ 都与 $\xi_1,\cdots,\xi_s$ 代数相关. 如果在同态 (16.7) 之下, 一个本身不为零的多项式 $f(\xi)$ 变为零, 那么我们可以在域 $K(\xi)$ 内将元素 $1/f$ 写成以下特殊形式：

$$\frac{1}{f(\xi_1,\cdots,\xi_n)}=\frac{g(\xi_1,\cdots,\xi_n)}{h(\xi_1,\cdots,\xi_s)}.$$

由此得

$$h(\xi_1,\cdots,\xi_s)=g(\xi_1,\cdots,\xi_n)f(\xi_1,\cdots,\xi_n).$$

在同态 (16.7) 之下, f 变为 0. 因此 $h(\xi_1,\cdots,\xi_s)$ 也一定变为 0, 这就是说, 我们有

$$h(\xi'_1,\cdots,\xi'_s)=0,$$

这与 $\xi'_1,\cdots,\xi'_s$ 的代数相关性的假设矛盾. 于是在同态 (16.7) 之下没有异于零的多项式被变为零. 从而 (16.7) 在 $r=s$ 时是一个同构. 这就得到 ξ' 是一个一般零点的论断.

$\mathfrak{p}$ 的每一个零点 ξ' 可以看成一个理想 $\mathfrak{p}'$ 的一般零点. 于是由 $f\equiv 0(\mathfrak{p})$ 得 $f(\xi')=0$ 或 $f\equiv 0(\mathfrak{p}')$. 从而 $\mathfrak{p}'$ 是 $\mathfrak{p}$ 的一个因子. 反过来 $\mathfrak{p}$ 的每一个异于 $\mathfrak{o}$ 的素因

① 这就是说, 它们可以通过使基域 K 的元素不动的同构互变.

子 $\mathfrak{p}'$ 都可以这样得到. 因为每一个理想 $\mathfrak{p}' \neq 0$ 都有一个一般零点 ξ'. 由刚才所述的定理, 立刻有

$\mathfrak{p}$ 的每一素因子 $\mathfrak{p}'$ 都具有维数 $r' \leqslant r$; 如果 $r' = r$, 那么必须 $\mathfrak{p}' = \mathfrak{p}$.

一个任意流形的维数指的是它的不可约成分中维数的最高的一个. 纯粹一维流形叫做曲线, 纯粹二维流形叫做曲面, 纯粹 $(n-1)$ 维流形叫做超曲面.

习题 16.2 一个主理想 (p), 这里 p 是一个不可分解的非常数多项式, 是一个 $(n-1)$ 维素理想.

习题 16.3 反过来, 每一 $(n-1)$ 维素理想都是主理想.

习题 16.4 $A_n(\Omega)$ 中唯一的 n 维流形就是 $A_n(\Omega)$ 本身; 属于它的理想是零理想.

16.5 Hilbert 零点定理, 齐次方程的结式组

每一个异于 $\mathfrak{o}$ 的素理想在泛域 Ω 内有一个一般零点. 因此一个没有零点的素理想就是单位理想 $\mathfrak{o}$.

我们现在一般地证明：

定理 *每一个在Ω内没有零点的理想 $\mathfrak{a} = (f_1, \cdots, f_r)$都是单位理想.*

证 假设存在一个理想 $\mathfrak{a} \neq \mathfrak{o}$ 没有零点. 于是根据极大原理, 存在一个极大理想 $\mathfrak{m} \neq \mathfrak{o}$ 也没有零点. 这个理想是无因子的, 从而根据 3.6 节是素的. 然而一个素理想 $\mathfrak{m} \neq \mathfrak{o}$ 总有零点.

上面所证明的定理也可以这样叙述：

定理 *如果多项式 $f_1, \cdots, f_r$ 在 $A_n(\Omega)$ 内没有公共零点, 那么等式*

$$1 = g_1 f_1 + \cdots + g_r f_r \tag{16.8}$$

成立.

这个定理是 Hilbert 零点定理的一个特殊情形. Hilbert 零点定理是说：

如果 f 是 $K[x_1, \cdots, x_n]$ 的一个多项式, 它在 $f_1, \cdots, f_r$ 在 $A_n(\Omega)$ 内的一切公共零点处都等于零, 那么

$$f^q = h_1 f_1 + \cdots + h_r f_r \tag{16.9}$$

对于某一自然数q成立.

证 通过 Rabinowitsch(*Mat. Ann.*, 102：518) 的巧妙办法, 这个一般情形将归结为刚才所证的特殊情形. 对于 $f = 0$, 断言是明显的. 在 $f \neq 0$ 的情形, 我们取一个新变量 z. 这时多项式

$$f_1, \cdots, f_r, 1 - zf$$

在 $A_{n+1}(\Omega)$ 内没有公共零点. 因此根据刚才所证明的定理, 有

$$1 = g_1 f_1 + \cdots + g_r f_r + g \cdot (1 - zf). \tag{16.10}$$

在这个恒等式里作代换 $z = 1/f$, 并且乘以某一幂 f^q 而消除由此所产生的分式. 得到

$$f^q = h_1 f_1 + \cdots + h_r f_r.$$

零点定理的推广　如果多项式 $p_1, \cdots, p_s$ 在 $f_1, \cdots, f_r$ 的一切公共零点处都等于零, 那么存在一个自然数 q, 使得 p_i 的一切 q 次幂积属于理想 $(f_1, \cdots, f_r)$ (反过来也成立).

证　有

$$p_i^{q_i} \equiv 0(f_1, \cdots, f_r).$$

令

$$q = (q_1 - 1) + (q_2 - 1) + \cdots + (q_s - 1) + 1.$$

于是每一幂积 $p_1^{h_1} \cdots p_s^{h_s}$, 其中 $h_1 + \cdots + h_s = q$, 至少含有一个因子 $p_i^{q_i}$. 因为不然的话 $h_1 + \cdots + h_s$ 最多将等于

$$(q_1 - 1) + \cdots + (q_s - 1) = q - 1.$$

于是得到这个断言. 逆命题是明显的.

作为最后所证的定理的应用, 我们导出齐式组, 即齐次多项式组 $F_1, \cdots, F_r$ 在域 Ω 内有非显易零点, 即有异于 $(0, \cdots, 0)$ 的零点所必须满足的条件.

如果 $(0, \cdots, 0)$ 是唯一的零点, 那么单项式 $x_1, \cdots, x_n$ 在理想 $(F_1, \cdots, F_r)$ 的一切零点处都将等于零, 从而由 $x_1, \cdots, x_n$ 所形成的每一个 q 次幂积 X_j 属于这个理想:

$$X_j = G_{j1} F_1 + \cdots + G_{jr} F_r. \tag{16.11}$$

设齐式 $F_1, \cdots, F_r$ 的次数为 $g_1, \cdots, g_r$. 在 (16.11) 式右端只保留 G_{ji} 中的 $q - g_i$ 次项而略去其他项, 就得到 (16.11) 式右端的 q 次项. 因此代替 G_{ij}, 得到一个 $q - g_i$ 次齐式 H_{ji}. 比较 (16.11) 式左右两端的 q 次项, 有

$$X_j = H_{j1} F_1 + \cdots + H_{jr} F_r. \tag{16.12}$$

反过来, 如果等式 (16.12) 对于一切 q 次幂积 X_j 成立, 那么 $(0, \cdots, 0)$ 是 $F_1, \cdots, F_r$ 的唯一公共零点.

x_j 的 $q - g_i$ 次幂积可以记作 X_{ki}. 在 (16.12) 中的 H_{ji} 是这些幂积的线性组合 (系数在 K 内). 因此 (16.12) 表明, 一切 q 次幂积 X_j 可以由乘积 $X_{ki} F_i$ 线性表示. 于是得到以下结果:

$F_1, \cdots, F_r$ 只有显易零点 $(0, \cdots, 0)$ 的充分且必要的条件是, 具有充分大的次数 q 的一切幂积 X_j 可以由乘积 $X_{ki}F_i$ 线性表示, 而系数取自K.

设 N_q 是 q 次幂积 X_j 的个数, 那么这个结果也可以这样叙述:

$F_1, \cdots, F_r$ 有一个非显易公共零点的充分且必要条件是, 对于每一 $q = 1, 2, \cdots$, 乘积 $X_{ki}F_i$ 中线性无关的个数小于 N_q.

把乘积 $X_{ki}F_i$ 表示成 X_j 的线性组合

$$X_{ki}F_i = \sum_j a_{kij}X_j,$$

那么对于每一 k 和 j, 由这些 a_{kij} 可以作出一个行向量

$$(a_{kil}, \cdots, a_{kiN}) \quad (N = N_q).$$

于是我们的条件就是说, 在这些行向量中线性无关的个数小于 N. 这就意味着, 由任意 N 个这样的行向量所组成的行列式应该等于零. 设 D_{qh} 是这样的行列式, 于是有

$F_1, \cdots, F_r$ 有一个非显易公共零点的充分且必要条件是

$$D_{qh} = 0 \quad (q = 1, 2, \cdots). \tag{16.13}$$

这里 a_{kij} 是齐式 F_i 的系数. 因此 D_{qh} 是齐式 $F_1, \cdots, F_r$ 的系数的整系数齐式.

首先假设 $F_1, \cdots, F_r$ 是次数为 $g_1, \cdots, g_r$ 的一般齐式, 因而带有真正不定系数 a_j, 于是我们有无限多个关于此系数的多项式 $D_{qh}(a_j)$. 然而根据 Hilbert 基定理, 在这些多项式中存在有限个, 而一切这样的多项式都可以由这有限个线性表示 (以整系数多项式作为系数). 如果 (对于特殊齐式 $F_1, \cdots, F_r$) 这有限个 D_{qh} 等于零, 那么一切 D_{qh} 都将是零, 从而方程组 $D_{qh} = 0$ 成立. 于是存在有限个 a_j 的整系数齐式

$$R_1(a_j), \cdots, R_m(a_j),$$

它们全等于零当且仅当齐式 $F_1, \cdots, F_r$ 有一个非显易公共零点[①].

具有上述性质的一个齐式组 $R_1, \cdots, R_m$ 叫做齐式 $F_1, \cdots, F_r$ 的结式组. 如果 F_i 是线性齐式, 那么由这 r 个齐式中每 n 个所能作成的 n 阶行列式构成一个结式组. 对于含两个变量 x_1, x_2 的两个齐式 F_1, F_2 来说, 通常的结式 R 就构成一个结式组. 同样地, 一般含 n 个变量的 n 个齐式有一个结式 R 就已足够. 参看 Hurwitz A. Über Trägheitsformen. *Ann. di Mat.* 3*a serie*, 1913, 20.

① 这个在代数几何中扮演着重要角色的定理是由 Mertens(Sitzungsber. *Wiener Akad.*, 108, S. 1174.) 提出的. 另一个证明由 Kapferer(Sitzungsber. *Bayer. Akad. München*, 1929: 179) 给出.

16.6 准素理想

多项式环里的理想论的主要问题是：判断一个多项式 f 是否属于一个给定的理想

$$\mathfrak{m} = (f_1, \cdots, f_r).$$

然而这里的所谓判断, 并不是指由有限个实际可行的运算构成的一个算法判断, 即使存在着这样的一个判断的话①, 而只是指这样的一个方法, 它同时给出关于理想的结构的一个详细考察, 并且使理想的零点与理想的元素 f 之间的几何关系尽可能清楚地表现出来. 这样的一个方法是由 Lasker 首先给出的②. 这个方法是通过将理想分解成准素分支而实现的.

Lasker 方法的主要思想如下：根据 15.4 节的分解定理, 每一个理想 $\mathfrak{m}$ 可以表示成准素理想的交：

$$\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_s].$$

因此, 一个多项式 f 属于这个理想 $\mathfrak{m}$ 必要且只要 f 属于一切准素理想 $\mathfrak{q}_\nu$. 因此, 为了在原则上解决上述问题, 只需建立一个多项式属于一个准素理想所必须满足的条件.

根据 15.3 节, 对于每一准素理想 $\mathfrak{q}$ 都有一个属于它的素理想 $\mathfrak{p}$ 以及一个指数 ρ 具有下列性质：

(1) $\mathfrak{p}^\rho \equiv 0(\mathfrak{q}) \equiv 0(\mathfrak{p})$;

(2) 由 $fg \equiv 0(\mathfrak{q})$ 及 $f \not\equiv 0(\mathfrak{p})$ 就有 $g \equiv 0(\mathfrak{q})$.

当 $\mathfrak{q} \neq \mathfrak{o}$, 素理想 $\mathfrak{p}$ 也属于一个不可约流形 M. 由 (1), $\mathfrak{q}$ 的一切零点同时也是 $\mathfrak{p}$ 的零点, 反过来也是如此. 因此, *一个准素理想 $\mathfrak{q} \neq \mathfrak{o}$ 的流形是不可约的并且等于属于它的素理想的流形.*

设 $\mathfrak{q}$ 是一个属于素理想 $\mathfrak{p}$ 的准素理想, 具有指数 ρ. M 是它的流形. 现在设 f 是包含 M 的一个多项式, 那么 $f \equiv 0(\mathfrak{p})$, 从而 $f^\rho \equiv 0(\mathfrak{q})$. 然而, 若 f 不包含 M, 那么根据上面的性质 (2), 在每一个模 $\mathfrak{q}$ 的同余式中可以将因子 f 去掉. 这是两个极重要的方法, 由此常常可以推导同余式 $f^\rho \equiv 0(\mathfrak{q})$ 或 $g \equiv 0(\mathfrak{q})$. 借助于分解定理可以立即转移到任意理想 $\mathfrak{m} = [\mathfrak{q}_1, \cdots, \mathfrak{q}_s]$ 上. 首先设 f 是一个多项式, 它包含 $\mathfrak{m}$ 的流形 M, 并且设 ρ 是准素理想 $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ 中指数最大的, 那么立即有

$$f^\rho \equiv 0(\mathfrak{q}_i) \quad (\text{对于} i = 1, \cdots, s),$$

① 参考 König. *Einleitung in die allgemeine Theorie der algebraischen Grössen.* Leipzig: B. G. Teubner, 1903 以及 Hermaun G. Die frage der endlich vielen schritte in der theorie der polynomideale. *Math. Ann.*, 95: 736–788.

② Lasker E. Zur theorie der moduln und ideale. *Math. Ann.*, 1905, 60: 20–116.

从而

$$f^\rho \equiv 0(\mathfrak{m}).$$

于是 Hilbert 零点定理 (16.5 节) 又重新被证明, 并且更加严格化, 即指数 ρ 只依赖于理想 $\mathfrak{m}$.

其次, 若 f 是一个多项式, 它不包含准素理想 $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ 的任何流形, 那么可以在每一同余式

$$fg \equiv 0(\mathfrak{m})$$

中将 f 约去而得到

$$g \equiv 0(\mathfrak{m}),$$

因为这个同余式对于一切准素理想 $\mathfrak{q}_\nu$ 成立. 这个约简的可能性又可以简单扼要地由方程

$$\mathfrak{m} : (f) = \mathfrak{m}$$

表示, 于是根据 15.5 节, 这个等式成立, 当且仅当 f 不能被所属的素理想 $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ 中的任何一个整除 (因而 f 不包含它们的不可约流形).

根据 15.5 节, 这个结果一般对于任意理想 $\mathfrak{a}$ 成立, 即

$$\mathfrak{m} : \mathfrak{a} = \mathfrak{m} \tag{16.14}$$

当且仅当 $\mathfrak{a}$ 不能被 $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ 中的任何一个整除, 换一句话说, 当且仅当 $\mathfrak{a}$ 的流形不包含素理想 $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ 的流形中的任一个. 这个定理在寻求属于一个给定理想 $\mathfrak{m}$ 的素理想 $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ 时常常是有用的. 这就是, 要推测素理想 $\mathfrak{p}$ 是否为素理想 $\mathfrak{p}_\nu$ 当中之一, 那么我们就取一个可以被 $\mathfrak{p}$ 整除的理想 $\mathfrak{a}$, 例如, $\mathfrak{a} = \mathfrak{p}$, 并且考察能否证明关系 (16.14) 成立或不成立, 即是否能由 $g\mathfrak{a} \equiv 0(\mathfrak{m})$ 为推出 $g \equiv 0(\mathfrak{m})$. 如果 (16.14) 成立, 那么 $\mathfrak{p}$ 不是任何 $\mathfrak{p}_\nu$.

所谓一个准素理想的维数指的是属于它的素理想的维数 (或流形的维数). 一个任意理想 $\mathfrak{a} \neq \mathfrak{o}$ 的维数或最高维数, 指的是它的准素分支 (或所属的素理想) 的维数中最高的. 如果属于 $\mathfrak{a}$ 的准素理想的维数都相等, 例如等于 d, 那么就称理想 $\mathfrak{a}$是纯d 维的.

习题 16.5 理想 (x_1^2, x_2x_3+1) 是准素的, 具有指数 2, 并且属于它的素理想是 (x_1, x_2x_3+1).

习题 16.6 一个不可分解, 非常数多项式 p 的每一幂 p^ρ 生成一个 $(n-1)$ 维准素理想. 每一个非常数多项式 f 生成一个纯 $(n-1)$ 维理想.

习题 16.7 设 $\mathfrak{p}$ 是习题 16.1 的素理想, 那么 $\mathfrak{p}^2$ 不是准素的 (多项式 $(x_2x^3-x_1^3)^2-(x_2^2-x_1x_3)(x_3^2-x_1^2x_2)$ 分裂出一个因子 x_1, 而其他因子不属于 $\mathfrak{p}^2$).

16.7 Noether 定理

借助于准素理想分解的方法, 我们首先就零维理想的情形解决为使一个多项式 f 属于一个理想 $\mathfrak{m}$, 这个多项式应该满足怎样的条件的问题. 我们从一个引理开始, 这个引理也常常是有用的:

引理　设 Σ 是 K 的一个扩域又设 $f, f_1, \cdots, f_r$ 是 $K[x] = K[x_1, \cdots, x_n]$ 的多项式, 那么由

$$f \equiv 0(f_1, \cdots, f_r) \quad 在\ \Sigma[x]\ 内$$

就得出

$$f \equiv 0(f_1, \cdots, f_r) \quad 在\ K[x] 内.$$

证　设

$$f = \sum g_i f_i, \tag{16.15}$$

这里 g_i 是系数在 Σ 内的多项式. 我们把这些系数用 Σ 的有限多个线性无关元素 $1, \omega_1, \omega_2, \cdots$ 线性表示, 系数取自 K. 这时 (16.15) 中每一项 $g_i f_i$ 都有形式

$$(g_{i0} + g_{i1}\omega_1 + g_{i2}\omega_2 + \cdots)f_i,$$

这里 g_{ik} 是系数在 K 内的多项式. 于是由 (16.15) 得出

$$f = \sum g_{i0}f_i + \omega_1 \sum g_{i1}f_i + \omega_2 \sum g_{i2}f_i + \cdots,$$

因为域元素 $1, \omega_1, \omega_2, \cdots$ 线性无关, 所以左右两端带有 $1, \omega_1, \omega_2, \cdots$ 的项必须对应地相等,

$$f = \sum g_{i0}f_i.$$

根据这个引理, 当我们要回答是否 $f \equiv 0(f_1, \cdots, f_r)$ 时, 总可以将基域 K 任意扩张, 例如, 通过添加理想 $(f_1, \cdots, f_r)$ 的零点而扩张. 如果所问的同余式在扩环 $\Sigma[x]$ 中成立, 那么它在扩张之前也成立.

一个零维流形在基域的适当扩张下总可以分解为一些单个的点. 因此, 为了方便起见, 我们总可以假设所出现的零维素理想各只有一个点作为零点 (而不像通常那样有一组共轭的零点).

一个零维素理想 $\mathfrak{p}$ 是无因子的. 因为根据 16.4 节, 同余类环 $\mathfrak{o}/\mathfrak{p}$ 是一个域. 因此每一个零维准素理想都是单素的. 因为根据 15.8 节, 一个准素理想, 当属于它的

素理想无因子时, 总是单素的. 由 15.8 节的定理还进一步得出, 一个理想 $\mathfrak{m}$ 的每一零维孤立准素分支 $\mathfrak{q}$ 可以表示为

$$\mathfrak{q} = (\mathfrak{m}, \mathfrak{p}^\rho), \tag{16.16}$$

这里的指数 ρ 是具有性质

$$\mathfrak{p}^\sigma \equiv 0(\mathfrak{m}, \mathfrak{p}^{\sigma+1}) \tag{16.17}$$

的数 σ 中最小的一个.

让我们将关系 (16.16) 的意义在基域已经事前如此扩张, 使得所考虑的单素理想 $\mathfrak{q}$ 各只有一个零点 $a = \{a_1, \cdots, a_n\}$ 的情形下, 再一次加以说明. (16.16) 是说, $f \equiv 0(\mathfrak{q})$ 必要且只要

$$f \equiv 0(\mathfrak{m}, \mathfrak{p}^\rho). \tag{16.18}$$

现在设 $\mathfrak{m}$ 通过一个基 $(f_1, \cdots, f_r)$ 给出, 并且假定 $y_\nu = x_\nu - a_\nu$, 那么 $\mathfrak{p} = (y_1, \cdots, y_n)$. 设想出现的一切多项式都按 y_ν 的升幂排列, 那么 $\mathfrak{p}^\rho$ 恰好由一切只含 y_ν 的次数 $\geqslant \rho$ 的幂积的多项式组成. 于是关系 (16.18) 就意味着, 除 ρ 次项及高于 ρ 次的项外, f 与一个线性组合 $\sum g_\nu f_\nu$ 一致. 这样, 如果我们设想将 $f_1, \cdots, f_r$ 乘以 1 以及诸 y_ν 的一切次数 $< \rho$ 的幂积, 并从此种乘积中略去一切次数 $\geqslant \rho$ 的项, 而将所得的多项式记作 $h_1, \cdots, h_k$, 那么 (16.18) 就是说, 除了次数 $\geqslant \rho$ 的项外, f 与 $h_1, \cdots, h_k$ 的一个带有常系数的线性组合相等. 这是一个事实, 它成立或不成立, 在所遇到每一情形下 (当 $\rho, f_1, \cdots, f_r$ 及 f 给定时) 都可以实际判定. 特别是当存在形式幂级数 $P_1(y), \cdots, P_r(y)$[①], 使得

$$f = P_1 f_1 + \cdots + P_r f_r \tag{16.19}$$

时[②], 这一事实成立. 这时对于 σ 的每一值, 我们可以去掉这些幂级数中从 σ 次项开始的一切项而保持等式 (16.19) 两端 mod $\mathfrak{p}^\sigma$ 一致. 因此这个幂级数判定标准实际上还是要求得过多一些: (16.19) 式两端不必完全一致, 而只需除去次数 $\geqslant \rho$ 的项外一致.

同样, 关系 (16.17) 对于每一 σ 成立与否是可以进行判断的: (16.17) 意味着, 一切 σ 次幂积都可以通过多项式 $\sum g_\nu f_\nu$ 去掉次数 $> \sigma$ 的幂积来表示. 因此我们可以就给定的 $f_1, \cdots, f_r$ 对于每一零点 a 逐个地检验值 $\sigma = 1, 2, 3, \cdots$, 直到求出一个使得 (16.17) 成立的 σ 为止, 这个 σ 就是 $\mathfrak{q}$ 的指数.

对于一个零维理想 $\mathfrak{m}$, 一切准素分支都是零维且孤立的. 因此我们可以将上述对于 $f \equiv 0(\mathfrak{q})$ 的判断标准应用到一切准素分支上. 如果这个判定标准对于一切零点都被满足, 那么由此就得到 $f \equiv 0(\mathfrak{m})$. 于是以下定理成立:

① 自然并不假定它们收敛.

② 这就是说, 在按 y_ν 的幂积形式地展开时, (16.19) 式两端一致.

定理 如果对于一个零维理想 $\mathfrak{m}$ 的每一零点 $a=\{a_1,\cdots,a_n\}$, 确定指数 ρ 为使得(16.17)对于 $\mathfrak{p}=(x_1-a_1,\cdots,x_n-a_n)$ 成立的最小自然数 σ, 又一个多项式 f 对于一切这样的 $\mathfrak{p}$ 满足条件(16.18), 那么 $f\equiv 0(\mathfrak{m})$.

这个定理对于 $\mathfrak{m}=(f_1,f_2)$, 其中 f_1,f_2 是两个变量的多项式的情形, 首先由 Noether 提出[①], 这就是著名的"Noether基本定理". 它是代数函数论中的"几何学方向"的基础. Noether 实际上代替较弱的关系 (16.18), 而假定幂级数条件 (16.19) 在一切零点处成立. 在这里的处理中, 只要求两端对 $y_1,\cdots,y_n$ 的到 $\rho-1$ 次为止的项一致. 这是由 Bertini 提出的[②], 同时他对于指数 ρ 也给出了一个界[③]. 对 n 维的推广则是由 Lasker 与 Macaulay 提出的. 使得 $f\equiv 0(\mathfrak{q})$ 的充分条件 $f\equiv 0(\mathfrak{m},\mathfrak{p}^\rho)$, 按照 Macaulay 的说法, 叫做在点 a 的 Noether 条件.

为了说明 Noether 定理的应用, 我们现在考虑一个特殊情形, 在这里 Noether 条件特别简单.

多项式 $f_1,\cdots,f_r$ 当中的每一个在 n 维空间里确定一个代数流形 (超曲面)$f_\nu=0$. 同样, 多项式 f 确定一个超曲面 $f=0$. 如果 f 分解成不可约因子: $f=p_1^{\rho_1}p_2^{\rho_2}\cdots$, 那么流形 $f=0$ 也分解成不可约部分 $p_1=0,p_2=0,\cdots$. 这里每一个不可约流形出现的次数按 f 的分解中相应的指数计.

如果将 f 对于一点 a 按 $y_\nu=x_\nu-a_\nu$ 的幂展开, 并且设展开式从 $s(s\geqslant 0)$ 次项开始:

$$f=c_0y_1^s+c_1y_1^{s-1}y_2+\cdots+c_\omega y_n^s+\cdots,$$

那么就说, 超曲面 $f=0$ 在 a*有一个*s*重点*. 命 s 次项 $c_0y_1^s+c_1y_1^{s-1}y_2+\cdots+c_\omega y_n^s$ 等于零, 可给出一个超曲面, 它是只由过 a 点的"直线"组成的, 称为超曲面 $f=0$ 在 a 点的**切锥**.

Noether 定理的最简单情形是, 在确定零维理想 $\mathfrak{m}$ 的超曲面 $f_1=0,\cdots,f_r=0$ 中, 有这样的超曲面 $f_1=0,\cdots,f_n=0$, 它们都以 a 为单点, 而它们的切超平面只有 a 点公共:

$$\begin{gathered}f_1=c_{11}y_1+\cdots+c_{1n}y_n+\cdots,\\ f_2=c_{21}y_1+\cdots+c_{2n}y_n+\cdots,\\ \cdots\cdots\cdots\\ f_n=c_{n1}y_1+\cdots+c_{nn}y_n+\cdots,\\ \text{线性型}\sum_{\mu=1}^n c_{\lambda\mu}y_\mu\text{线性无关.}\end{gathered}$$

① Noether M. Über einen satz aus der theorie der algebraischen funktionen. *Math. Ann.*, 1873, 6: 351–359.

② Bertini E. Zum fundamentalsatz aus der theorie der algebraischen funktionen. *Math. Ann.*, 1889, 34: 447–449.

③ 较严格的界由 Dubreil P. *These de Doctorat.* Paris, 1930 给出.

在这个情形, 如果将素理想 $(x_1-a_1,\cdots,x_n-a_n)$ 记作 $\mathfrak{p}$, 那么 $y_1,\cdots,y_n$ 本身也出现在 $f_1,\cdots,f_n$ 的 mod $\mathfrak{p}^2$ 线性组合 (即略去二次及高次项) 中, 这就是说,

$$(y_1,\cdots,y_n)\equiv 0((f_1,\cdots,f_n),\mathfrak{p}^2),$$

从而

$$\mathfrak{p}\equiv 0(\mathfrak{m},\mathfrak{p}^2).$$

由此得出, 理想 $\mathfrak{m}$ 在点 a 有一个指数为 1 的孤立准素分支 $\mathfrak{q}$, 即 $\mathfrak{q}=\mathfrak{p}$. 因此每一个以 a 为零点的多项式可以被 $\mathfrak{q}$ 整除.

关于 Noether 定理的其他特殊情形及应用, 可参看作者本人的*Einführung in die Algebraische Geometrie* (Springer, 1939 年出版).

16.8 多维理想归结到零维理想

在这一节里, 我们打算把在 16.7 节里对于零维理想所证明的定理扩充到多维理想上.

方法如下: 设 $\mathfrak{q}$ 是 $K[x]$ 中一个 d 维准素理想, $\mathfrak{p}$ 是属于它的素理想, $\{\xi_1,\cdots,\xi_n\}$ 是它的一般零点, 又设 (例如) $\xi_1,\cdots,\xi_d$ 是代数无关的, 那么可以通过代换 $x_1=\xi_1,\cdots,x_d=\xi_d$ 将理想 $\mathfrak{q}$ 与 $\mathfrak{p}$ 化为零维理想. 我们对理想 $\mathfrak{q}$ 的一切多项式 g 施行这个代换. 于是多项式 q 变为 $K(\xi_1,\cdots,\xi_d)[x_{d+1},\cdots,x_n]$ 中的多项式 q', 它们生成一个理想 $\mathfrak{q}'$. 显然只需对基多项式 $q_1,\cdots,q_r$ 施行代换 $x_1=\xi_1,\cdots,x_d=\xi_d$ 就够了. 这时对应的多项式 $q_1',\cdots,q_r'$ 生成理想 $\mathfrak{q}'$:

$$\mathfrak{q}'=(q_1',\cdots,q_r').$$

理想 $\mathfrak{q}'$ 显然由多项式 q' 除以 $\xi_1,\cdots,\xi_d$ 的任意异于零的多项式 φ 所组成, 因为多项式 q' 在 $K[\xi_1,\cdots,\xi_d,x_{d+1},\cdots,x_n]$ 中作成一个理想, 并且为了得到它们在 $K(\xi_1,\cdots,\xi_d)[x_{d+1},\cdots,x_n]$ 所生成的理想, 只要容许带有分母 φ 即可.

如同由 $\mathfrak{q}$ 产生 $\mathfrak{q}'$ 的方法那样, 由 $\mathfrak{p}$ 可以产生一个理想 $\mathfrak{p}'$, 并且一般地由每一理想 $\mathfrak{m}=(f_1,\cdots,f_r)$ 可以产生一个理想 $\mathfrak{m}'=(f_1',\cdots,f_r')$.

代换 $x_1=\xi_1,\cdots,x_d=\xi_d$ 的几何意义, 是用通过 $\mathfrak{q}$ 的流形的一般点的线性空间 $x_1=\xi_1,\cdots,x_d=\xi_d$ 去截这个流形.

设 $f(x_1,\cdots,x_n)$ 是一个多项式, 而 $f(\xi_1,\cdots,\xi_d,x_{d+1},\cdots,x_n)$ 属于 $\mathfrak{q}'$, 那么根据上述,

$$f(\xi,x)=\frac{q'}{\varphi(\xi_1,\cdots,\xi_d)}=\frac{q(\xi,x)}{\varphi(\xi)},\quad \text{其中} q(x)\equiv 0(\mathfrak{q}),$$

从而

$$q(\xi,x)=\varphi(\xi)f(\xi,x).$$

于是, 由 $\xi_1,\cdots,\xi_d$ 的代数无关性推出

$$q(x)=\varphi(x)f(x)\equiv 0(\mathfrak{q}).$$

然而, 若 $\varphi(\xi)\neq 0$, 则 $\varphi(x)\not\equiv 0(\mathfrak{p})$, 从而

$$f(x)\equiv 0(\mathfrak{q}).$$

因此, 为了判断一个多项式 $f(x)$ 是否属于 $\mathfrak{q}$, 只需研究对应的 $f'=f(\xi_1,\cdots,\xi_d,x_{d+1},\cdots,x_n)$ 是否属于 $\mathfrak{q}'$. 于是 $\mathfrak{q}'$ 唯一确定 $\mathfrak{q}$.

我们现在断言:

定理 理想 $\mathfrak{q}'$在$K(\xi_1,\cdots,\xi_d)[x_{d+1},\cdots,x_n]$中是准素的; 属于它的素理想是 $\mathfrak{p}'$; $\mathfrak{q}'$ 的指数等于 $\mathfrak{q}$ 的指数; $\mathfrak{p}'$ 的一般零点是$\{\xi_{d+1},\cdots,\xi_n\}$, 且 $\mathfrak{p}'$的维数是零.

证 为了证明 $\mathfrak{q}'$ 是准素的而 $\mathfrak{p}'$ 是属于它的素理想, 只需证明下列三个性质:

(1) 由 $f(\xi,x)g(\xi,x)\equiv 0(\mathfrak{q}')$ 及 $f(\xi,x)\not\equiv 0(\mathfrak{p}')$ 就有 $g(\xi,x)\equiv 0(\mathfrak{q}')$;

(2) 由 $f(\xi,x)\equiv 0(\mathfrak{q}')$ 就有 $f(\xi,x)\equiv 0(\mathfrak{p}')$;

(3) 由 $f(\xi,x)\equiv 0(\mathfrak{p}')$ 就有 $f(\xi,x)^\rho\equiv 0(\mathfrak{q}')$.

在所有这三个性质中都可以假定 f 与 g 是 $\xi_1,\cdots,\xi_d$ 的有理整函数, 因为在其他情形只要乘以一个适当的多项式 $\varphi(\xi)$ 即可. 于是根据上面的注记, 一般可以用 x 代替 ξ, 用 $\mathfrak{q}$ 代替 $\mathfrak{q}'$, 用 $\mathfrak{p}$ 代替 $\mathfrak{p}'$. 这是因为 $f(\xi,x)\equiv 0(\mathfrak{q}')$ 与 $f(x)\equiv 0(\mathfrak{q})$ 等价, 等等. 然而在这样代替之下, (1)~(3) 所说的不是别的, 就是 $\mathfrak{q}$ 是准素的而 $\mathfrak{p}$ 是属于它的素理想, 这一点是我们已知的. 同时也证明了, $\mathfrak{q}'$ 与 $\mathfrak{q}$ 的指数相同.

为了证明 $\{\xi_{d+1},\cdots,\xi_n\}$ 是 $\mathfrak{p}'$ 的一般零点, 我们只需证明, 如果

$$f(\xi_1,\cdots,\xi_d,\xi_{d+1},\cdots,\xi_n)=0,$$

这里 f 对于 $\xi_1,\cdots,\xi_d$ 是有理的而对于 $\xi_{d+1},\cdots,\xi_n$ 是有理整的, 那么

$$f(\xi,x)\equiv 0(\mathfrak{p}'),$$

并且反过来也成立. 我们还可以进一步假定 f 对于 $\xi_1,\cdots,\xi_d$ 也是整的. 然而这时 $f(\xi,x)\equiv 0(\mathfrak{p}')$ 与 $f(x)\equiv 0(\mathfrak{p})$ 等价. 因此, 注意到 $\{\xi_1,\cdots,\xi_n\}$ 是 $\mathfrak{p}$ 的一般零点, 断言的这一部分也被证明.

最后, 由于 $\{\xi_{d+1},\cdots,\xi_n\}$ 对于 $K(\xi_1,\cdots,\xi_d)$ 来说是代数的, 所以 $\mathfrak{p}'$ 的维数是零. 这样, 一切论断都被证明.

用同样的方法也可以证明, 如果 $\mathfrak{q}$ 是理想 $\mathfrak{m}=(f_1,\cdots,f_r)$ 的一个准素分支, 那么 $\mathfrak{q}'$ 也是对应的理想 $\mathfrak{m}'=(f_1',\cdots,f_r')$ 的一个准素分支. 如果 $\mathfrak{q}$ 是 $\mathfrak{m}$ 的一个孤立分支, 那么 $\mathfrak{q}'$ 也是 $\mathfrak{m}'$ 的一个孤立分支.

将一切准素理想化为零维理想所发展的方法使我们掌握一个工具, 用来对每个给定的的多项式 f 来判断它是否属于一个给定的理想 $\mathfrak{m}=(f_1,\cdots,f_r)$. 预先假定 $\mathfrak{m}$ 已经被分解为准素分支:

$$\mathfrak{m}=[\mathfrak{q}_1,\cdots,\mathfrak{q}_s].$$

对于每一个准素分支 $\mathfrak{q}$ 求出相应的零维理想 $\mathfrak{q}'$, 然后将域扩张为 $K(\xi_1,\cdots,\xi_d)$, 使得 $\mathfrak{q}'$ 分解为准素理想 $\mathfrak{q}_\nu'$, 其中每一 $\mathfrak{q}_\nu'$ 只有一个零点 $a^{(\nu)}$, 再根据 16.7 节所述的方法, 利用 "Noether 条件"

$$f'\equiv 0(\mathfrak{q}',\mathfrak{p}_\nu'^{\rho}),\mathfrak{p}'_\nu=(x_{d+1}-a_{d+1}^{(\nu)},\cdots,x_n-a_n^{(\nu)}) \tag{16.20}$$

来研究多项式 f' 是否属于理想 $\mathfrak{q}_\nu'=(\mathfrak{q}',\mathfrak{p}_\nu'^{\rho})$, 从而是否属于理想 $\mathfrak{q}'$. 因为 $\mathfrak{p}_\nu'$ 的零点对于 $K(\xi_1,\cdots,\xi_d)$ 共轭, 所以 $\mathfrak{p}_\nu'$, 从而 $\mathfrak{q}_\nu'$ 也对于 $K(\xi_1,\cdots,\xi_d)$ 共轭. 因此只需对每一 $\mathfrak{q}'$ 研究一个$\mathfrak{q}_\nu'$ 即可. 这样, 我们只需添加每一 $\mathfrak{q}'$ 的一个零点. 设 $\{\xi_{d+1},\cdots,\xi_n\}$ 是这样一个零点. 于是 $\mathfrak{p}_\nu'$ 就被素理想

$$\mathfrak{p}_\xi=(x_{d+1}-\xi_{d+1},\cdots,x_n-\xi_n)$$

所代替, 而代替条件 (16.20), 我们可以利用较方便的条件

$$f'\equiv 0(\mathfrak{m}',\mathfrak{p}_\xi^{\rho}). \tag{16.21}$$

因为 (16.21) 对于 $f\equiv 0(\mathfrak{m})$ 来说也是必要的, 并且由 (16.21) 立即得 (16.20). $\mathfrak{m}$ 的每一准素分支所必须满足的条件 (16.21) 叫做 Hentzeit 判定标准或 Hentzeit 零点定理.

特别, 若 $\mathfrak{q}$ 是 $\mathfrak{m}$ 的一个孤立分支, 那么 $\mathfrak{q}'$ 也是 $\mathfrak{m}'$ 的一个孤立分支, 于是我们可以像 15.8 节那样由条件

$$\mathfrak{p}_\xi^{\rho}\equiv 0(\mathfrak{m}',\mathfrak{p}_\xi^{\rho+1})$$

来确定指数 ρ.

由条件 (16.20), 对于 $f\equiv 0(\mathfrak{q})$ 最清楚地揭示出准素理想固有的几何意义：为了使多项式 f 属于一个准素理想, 常常要对于 f 在一个不可约流形的一个一般点 ξ 按 $x_1-\xi_1,\cdots,x_n-\xi_n$ 的展开式的首项附加某种要求, 例如, 要求 f 在这个一般点等于零, 或者要求超曲面 $f=0$ 在这个一般点与另一包含 M 的超曲面相切, 等等.

习题 16.8　利用化为零维理想的方法证明, $K[x_1,\cdots,x_n]$ 中每一 $(n-1)$ 维准素理想都是主理想.

习题 16.9　$K[x_1,\cdots,x_n]$ 中每一纯 $(n-1)$ 维理想都是主理想, 反过来也对.

第 17 章　代 数 整 量

在历史上, 理想论的发展有两个出发点：代数整数论及多项式理想论. 这两个理论各自从完全不同的问题展开. 在多项式理想方面以零点的决定和关于一个多项式属于一个理想的充分必要条件的建立作为中心问题, 而在代数整数论方面则从因子分解的问题向前发展. 让我们通过以下的考察来说明这个问题是如何形成的.

在数 $a+b\sqrt{-5}$ 的环里, 其中 a 与 b 都是有理整数, 元素的唯一分解定理不成立. 例如, 9 容许两种本质上不同的不可约因子分解[①]：

$$9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5}).$$

这一事实促使 Dedekind (仿照 Kummer 对于分圆域通过引入某种“理想数”而强制得到因子分解的唯一性的办法) 将元素的领域扩充到 (他所首先命名的) 理想的领域. 于是他可以证明, 在这样的领域里, 每一个理想都等于素理想的唯一确定的乘积. 事实上, 在上述情形, 如果引入素理想

$$\mathfrak{p}_1=(3,2+\sqrt{-5}),\quad \mathfrak{p}_2=(3,2-\sqrt{-5}),$$

我们就很容易验证：

$$(3)=\mathfrak{p}_1\mathfrak{p}_2,\quad (2+\sqrt{-5})=\mathfrak{p}_1^2,\quad (2-\sqrt{-5})=\mathfrak{p}_2^2,$$

从而对于主理想 (9), 我们得到唯一的分解

$$(9)=\mathfrak{p}_1^2\mathfrak{p}_2^2.$$

在这一章里, 一个域的整量的“古典”(Dedekind) 理想论将按近代的, 由 Noether[②]所拟定的公理形式来阐述. 在叙述中并不假定第 13 章的一般理想论, 虽然也将常常涉及它们的相互关系.

---

① 数 3 与 $2\pm\sqrt{-5}$ 的不可约性容易由它们的范数 (参看 6.11 节) 是 9 得出. 如果它们可分解, 那么必定或者两个因子有范数 ± 3, 或者一个因子有范数 ± 1. 具有范数 ± 3 的数 $a+b\sqrt{-5}$ 是不存在的, 因为这时必须有

$$a^2+5b^2=\pm 3,$$

这在整数里面是不可能的. 一个具有范数 ± 1 的数必定是可逆元素 ± 1 之一, 因为

$$a^2+5b^2=\pm 1$$

仅能被 $a=\pm 1$ 且 $b=0$ 所满足.

② Noether E. Abstrakter Aufbau der Idealtheorie in algebraischen Zahl und Funktionenkörpern. *Math. Ann.*, 1926, 96：26—61.

17.1 有限 $\mathfrak{R}$ 模

我们考虑关于一个 (不一定交换) 环 $\mathfrak{R}$ 的模, 这就是说, 以 $\mathfrak{R}$ 作为 (左) 乘子区的模. 通常所考虑的模多半或者包含在 $\mathfrak{R}$ 内 (因而是 $\mathfrak{R}$ 的左理想) 或者在一个扩环 $\mathfrak{S}$ 内.

所谓一个有限 $\mathfrak{R}$ 模, 指的是一 $\mathfrak{R}$ 模 $\mathfrak{M}$, 它是由一个有限模基 $(a_1, \cdots, a_h)$ 生成的, 换句话说, 它的元素都可以由 $a_1, \cdots, a_h$ 线性表示, 而系数取自 $\mathfrak{R}$ 或为整数:

$$m = r_1 a_1 + \cdots + r_h a_h + n_1 a_1 + \cdots + n_h a_h \quad (r_\nu \in \mathfrak{R}, n_\nu\text{是整数}). \tag{17.1}$$

在这一情形我们记 $\mathfrak{M} = (a_1, \cdots, a_h)$.

我们说, 对于一个模 $\mathfrak{M}$因子链条件成立. 如果 $\mathfrak{M}$ 的子模 $\mathfrak{M}_1, \mathfrak{M}_2, \cdots$ 的每一个链, 其中每一个后面的都真正包含它的前一个 (是前一个的真“因子”):

$$\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset \cdots$$

在有限步后终止.

定理 *如果因子链条件对于 $\mathfrak{M}$ 成立, 那么 $\mathfrak{M}$ 的每一个子模都有一个有限基, 并且反过来也成立.*

这个定理是 15.1 节关于理想基与因子链条件的定理的一般化. 证明完全类似.

为了找出子模 $\mathfrak{N}$ 的一个基, 我们首先在 $\mathfrak{N}$ 里找出一个元素 a_1. 如果 $(a_1) = \mathfrak{N}$, 那么已经完成. 假定在 $\mathfrak{N}$ 里还有一个元素 a_2, 而 a_2 不属于 (a_1). 若 $(a_1, a_2) = \mathfrak{N}$, 那么已经完成. 否则再求出一个元素 a_3, 如此等等. 如果已知模链

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

在有限多项必须终止, 那么 $\mathfrak{N}$ 有一个有限基.

反过来, 如果 $\mathfrak{M}$ 的每一个子模都有一个有限基, 而

$$\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset \cdots$$

是 $\mathfrak{M}$ 的子模的一个因子链, 那么一切 $\mathfrak{M}_\nu$ 的并 $\mathfrak{B}$ 仍是一个子模, 它也有一个有限基:

$$\mathfrak{B} = (a_1, \cdots, a_r).$$

然而一切 a_ν 已经包含在这个链的某一个 $\mathfrak{M}_\omega$ 里, 因此 $\mathfrak{B} \subseteq \mathfrak{M}_\omega$, 从而 $\mathfrak{B} = \mathfrak{M}_\omega$. 于是这个链在 $\mathfrak{M}_\omega$ 处终止.

在怎样的条件下因子链条件对于 $\mathfrak{M}$ 确实成立, 由以下定理指出:

定理　如果在 $\mathfrak{R}$ 里因子链条件对于左理想成立, 而 $\mathfrak{M}$ 是一个有限 $\mathfrak{R}$ 模, 那么在 $\mathfrak{M}$ 中因子链条件对于 $\mathfrak{R}$ 模成立.

于是这一命题等价于 (基于以上定理):

定理　如果在 $\mathfrak{R}$ 内每一个左理想都有一个有限理想基, 而 $\mathfrak{M}$ 有一个有限$\mathfrak{R}$模基, 那么 $\mathfrak{M}$ 的每一个子模也有一个有限 $\mathfrak{R}$ 模基.

证明与 Hilbert 基定理 (15.1 节) 的证明完全类似. 设 $\mathfrak{M} = (a_1, \cdots, a_h)$, 又设 $\mathfrak{N}$ 是 $\mathfrak{M}$ 的一个子模. $\mathfrak{N}$ 的每一个元素可以写成形式 (17.1). 如果在表示式 (17.1) 里的 $2h$ 个系数 $r_1, \cdots, n_h$ 中后 $2h - l$ 个, 即由第 $l + 1$ 到第 $2h$ 个, 系数都是零, 那么就说这个表示式有长度$\leqslant l$. 我们现在考虑出现在 $\mathfrak{N}$ 里, 长度 $\leqslant l$ 的一切表示式. 我们立即看出, 它们的第 l 个系数 (r_l或n_{l-h}) 作成 $\mathfrak{R}$ 或整数环 $\mathbb{Z}$ 中的一个左理想. 这个理想有一个有限基

$$(b_{l1}, \cdots, b_{ls_l}).$$

每一 $b_{l\nu}$ 都是某一个表示式 (17.1) 的最后 (第 l 个) 系数 (r_l或n_{l-h}), 我们把这个表示式记作 $B_{l\nu}$:

$$B_{l\nu} = r_1a_1 + \cdots + b_{l\nu}a_l \quad 或 = r_1a_1 + \cdots + b_{l\nu}a_{l-h}.$$

我们断言, 一切这样的 $B_{l\nu}(l = 1, \cdots, 2h; \nu = 1, \cdots, s_l)$ 在一起作成 $\mathfrak{N}$ 的一个基. 事实上, $\mathfrak{N}$ 的每一个长度为 l 的元素 (17.1) 可以通过减去一个 $B_{l11}, \cdots, B_{ls_l}$ 的线性组合 (系数在 $\mathfrak{R}$ 或 $\mathbb{Z}$ 内, 由 l 而定) 而将它的最后 (第 l 个) 系数消去, 这就是说, 化为一个长度较短的表示式; 后者又可以按同样办法将它的长度缩短, 直到经过逐次减去 $B_{l\nu}$ 的线性组合最后剩下的是零为止. 于是 $\mathfrak{N}$ 的每一个元素可以写成 $B_{l\nu}$ 的线性组合. 证毕.

如果理想 $(b_{l1}, \cdots, b_{ls_l})$ 的某一个是零理想, 那么对应的 $B_{l\nu}$ 在这个基里是完全多余的.

17.2　关于一个环的整量

设 $\mathfrak{R}$ 是环 $\mathfrak{T}$ 的一个子环.

$\mathfrak{T}$ 的一个元素 t 叫做关于 $\mathfrak{R}$ 是整的, 如果 t 的一切幂[①]都属于一个有限 $\mathfrak{R}$ 模 $(a_1, \cdots, a_m)$, 或者, 如果 t 的一切幂都可以由 $\mathfrak{T}$ 的有限个元素 $a_1, \cdots, a_m$ 线性地表示成

$$t^\rho = r_1a_1 + \cdots + r_ma_m + n_1a_1 + \cdots + n_ma_m \quad (r_\nu \in \mathfrak{R}, n_\nu 是整数) \tag{17.2}$$

① 在这一节里, 关于幂都只理解为具有正指数.

的形式.

特别, $\mathfrak{R}$ 的每一元素 r 关于 $\mathfrak{R}$ 都是整的, 因为 $r, r^2, r^3, \cdots$ 都属于 $\mathfrak{R}$ 模 (r). $\mathfrak{T}$ 的单位元, 如果存在的话, 关于 $\mathfrak{R}$ 总是整的.

如果 $\mathfrak{T}$ 是一个域, 那么它包含 $\mathfrak{R}$ 的商域 P, 于是一个整量 t 的一切幂都与有限个元素 $a_1, \cdots, a_m$ 线性相关, 系数在 P 内. 因为 P 非但包含环 $\mathfrak{R}$, 而且还含有单位元. 因此在 t 的幂中只有有限多个关于 P 线性无关. 所以 t 是 P 上的代数元. 因此, 代替"整量"也可以说代数整量.

如果 $\mathfrak{R}$ 是一个环, 在其中因子链条件成立, 那么由 17.1 节, 因子链条件对于有限 $\mathfrak{R}$ 模 $(a_1, \cdots, a_m)$ 的子模也成立. 特别, 模的链

$$(t) \subseteq (t, t^2) \subseteq \cdots$$

不能由完全不同的模组成, 这就是说, t 的某一个幂可以由较低次幂线性表示:

$$t^h = r_1 t + \cdots + r_{h-1} t^{h-1} + n_1 t + \cdots + n_{h-1} t^{h-1}. \tag{17.3}$$

反过来, 如果 t 是 $\mathfrak{T}$ 的一个元素, 它对于某一适当的 h 容许一个形式如 (17.3) 而系数在 $\mathfrak{R}$ 或 $\mathbb{Z}$ 内的表示式, 那么逐次利用 (17.3), t 的一切较高次的幂都可以由有限个 $t, t^2, \cdots, t^{h-1}$ 线性表示, 从而根据我们的定义, t 是整的. 这样就证明了:

定理　*如果在环 $\mathfrak{R}$ 内, 因子链条件对于左理想成立, 那么 t 关于 $\mathfrak{R}$ 是整的, 其必要且充分的条件是有一个形式如 (17.3) 的方程存在.*

当 $\mathfrak{T}$ 是一个域时, 方程 (17.3) 又带来了 t 是代数元的一个新的意义. 如果 $\mathfrak{R}$ 有单位元, 那么对于 t 的幂还可以添上 $t^0 = 1$, 此外, 在 (17.3) 里还可以去掉尾项 $n_1 t + \cdots + n_{h-1} t^{h-1}$. 从而代替 (17.3) 我们得到一个较简单的方程

$$t^h - r_{h-1} t^{h-1} - \cdots - r_0 = 0,$$

它的特征是 t 的最高次幂的系数是 1.

例　代数整数是这样的代数数, 它们关于通常的整数环 $\mathbb{Z}$ 是整的, 因而满足一个最高系数是 1 的整系数方程. $x_1, \cdots, x_n$ 的代数整函数是 $K(x_1, \cdots, x_n)$ 的一个代数扩域内的这样的函数, 它们关于多项式环 $K[x_1, \cdots, x_n]$ 是整的. 此处 K 是一个取定的域. $x_1, \cdots, x_n$ 的绝对代数整函数是这样的函数, 它们关于整系数多项式环 $\mathbb{Z}[x_1, \cdots, x_n]$ 是整的.

在一个交换环 $\mathfrak{T}$ 里, 两个关于 $\mathfrak{R}$ 的整量的和, 差与积仍然是整的. 或者说, $\mathfrak{T}$ 中关于 $\mathfrak{R}$ 的整量作成一个环 $\mathfrak{S}$.

证　如果 s 的一切幂可以由 $a_1, \cdots, a_m$ 线性表示, 并且 t 的一切幂可以由 $b_1, \cdots, b_n$ 线性表示, 那么 $s+t, s-t$ 或 $s \cdot t$ 的一切幂可以由 $a_1, \cdots, a_m, b_1, \cdots, b_n, a_1 b_1, a_1 b_2, \cdots, a_m b_n$ 线性表示.

我们现在假定因子链条件对于环 $\mathfrak{S}$ 的理想成立, 那么就可以证明:

整性的传递性定理 设 $\mathfrak{S}$ 是交换环 $\mathfrak{T}$ 中(关于子环 $\mathfrak{R}$ 的)整量所成的环, 又设 $\mathfrak{T}$ 的元素 t 关于$\mathfrak{S}$是整的, 那么 t 关于 $\mathfrak{R}$ 也是整的(即属于 $\mathfrak{S}$). 换一句话说, 如果 t 满足一个形式如(17.3)的方程, 它的系数 r_ν 关于 $\mathfrak{R}$ 是整的, 那么 t 本身关于 $\mathfrak{R}$ 也是整的.

证 通过累次应用方程 (17.3), 可以将一切幂 $t^{h+\lambda}$ 由 $t,t^2,\cdots,t^{h-1}$ 线性表示, 系数或者是整数或者由 r_ν 的幂积有理整地表示. 对于每一 r_ν, 存在 $\mathfrak{T}$ 中有限个量, 使得 r_ν 的一切幂都可以由这些量线性表示, 而系数或者属于 $\mathfrak{R}$ 或者是整数. 于是 r_ν 的一切幂积都可以由这有限个量的有限个乘积线性表示. 用 $t,t^2,\cdots,t^{h-1}$ 乘这有限个乘积, 最后也将 $t,t^2,\cdots,t^{h-1}$ 取在内, 那么仍然得到有限个量, 而 t 的一切幂都可以由这些量线性表示, 系数或者属于 $\mathfrak{R}$, 或者是整数.

一个环 $\mathfrak{S}$ 叫做在一个扩环 $\mathfrak{T}$ 内整闭的, 如果 $\mathfrak{T}$ 的每一个关于 $\mathfrak{S}$ 的整量都属于 $\mathfrak{S}$. 特别, 一个整环 $\mathfrak{S}$, 如果在它的商域 Σ 内是整闭的, 那么就简称为整闭的. 容易看出, 这就意味着, 对于 Σ 的任意元素 t, 如果它的一切幂 t^ρ 都可以表示成分数, 并且分母为 $\mathfrak{S}$ 中的确定元素, 那么 t 本身属于 $\mathfrak{S}$. 实际上, 能够用来表示一个整量 t 的一切幂的有限个量总可以化为有公分母的分数, 反过来, 如果 t 的一切幂都可以表示成分母为 s 的分数, 那么它们都可以由一个量 s^{-1} 线性表示.

由以上的定理得出, 在 $\mathfrak{T}$ 的交换性的假定下, $\mathfrak{T}$ 中关于 $\mathfrak{R}$ 的一切整量所成的环 $\mathfrak{S}$, 当因子链条件对于 $\mathfrak{S}$ 的理想成立时, 在 $\mathfrak{T}$ 中总是整闭的.

同一定理也可以在没有因子链条件的假定下来证明, 如果代替这个条件, 假定 $\mathfrak{R}$ 在它的商域 P 内是整闭的而 $\mathfrak{T}$ 是 P 的一个有限扩域. 为了证明这一结论, 将 $\mathfrak{T}$ 扩张成为 P 上的一个正规扩域 $\mathfrak{T}'$, 并且将 $\mathfrak{S}$ 扩张成为 $\mathfrak{T}'$ 的整量所成的环 $\mathfrak{S}'$. 如果一个元素 t 关于 $\mathfrak{S}$ 是整的, 那么关于 $\mathfrak{S}'$ 也是整的, 于是 t 的共轭量 (关于 P 的) 从而这些共轭量的初等对称函数, 即 t 的定义方程的系数, 关于 $\mathfrak{S}'$ 也是整的. 于是根据 $\mathfrak{R}$ 的整闭性, 这些系数属于 $\mathfrak{R}$, 从而 t 关于 $\mathfrak{R}$ 是整的, 因此 $t\in\mathfrak{S}$.

对于一个整环的整闭性的一个充分但非必要的判定标准由以下定理给出:

定理 一个有单位元的整环, 如果在其中元素的唯一素因子分解定理成立, 那么在它的商域内是整闭的.

证 商域的每一元素可以表成这样的分数 a/b, 其中 a 与 b 没有公共素因子. 于是, 如果要将 a/b 的一切幂都乘以单独一个量 c 而把分母去掉, 那么 ca^n, 从而 c 必须对于一切 n 来说都能被 b^n 整除, 这只有在 b 是一个可逆元素, 从而 $\dfrac{a}{b}=ab^{-1}$ 属于整环时才可能.

由这个定理得出, 一切主理想环 (特别整数环 $\mathbb{Z}$), 每一个整系数多项式环以及每一域 K 上的多项式环都是整闭的.

习题 17.1 一个域的单位根对于每一子环来说总是整的.

习题 17.2　Gauss 数域 $\mathbb{Q}(i)$ 中什么样的数关于 $\mathbb{Z}$ 是整的? 域 $\mathbb{Q}(\rho)$ 中什么样的数关于 $\mathbb{Z}$ 是整的, 这里 $\rho=-\dfrac{1}{2}+\dfrac{1}{2}\sqrt{-3}$ 是一个三次单位根?

习题 17.3　如果整环 $\mathfrak{R}$ 是整闭的, 那么多项式环 $\mathfrak{R}[x]$ 也是整闭的.

17.3　一个域的整量

设 $\mathfrak{R}$ 是一个整环, P 是它的商域, Σ 是 P 的一个有限扩域而 $\mathfrak{S}$ 是 Σ 中关于 $\mathfrak{R}$ 的整量所成的环. 显然 $\mathfrak{S}$ 是 $\mathfrak{R}$ 的一个扩环. 我们可以将环 $\mathfrak{R}$, $\mathfrak{S}$ 与域 P, Σ 之间的关系用图来表示:

$$\begin{array}{ccc}\mathfrak{R} & \subseteq & \mathfrak{S}\\ \cap & & \cap\\ P & \subseteq & \Sigma.\end{array}$$

在这一节里, 这些关系都是固定的. 说到"整"时总意味着: 关于 $\mathfrak{R}$ 是整的.

例　设 $\mathfrak{R}$ 是通常的整数环, 于是 P 是有理数域, Σ 是一个数域 (对于 P 是有限的), 而 $\mathfrak{S}$ 是 Σ 的代数整数所成的环.

如果 $\mathfrak{R}$ 是一个多项式环: $\mathfrak{R}=K[x_1,\cdots,x_n]$, 那么 P 就是有理函数域; Σ 是由 P 通过添加有限个代数函数组成的, 而 $\mathfrak{S}$ 是域 Σ 中的代数整函数; 等等.

我们的目的是研究 $\mathfrak{S}$ 中的理想理论. 如我们所知, 首先需要研究的是, 对于 $\mathfrak{S}$ 的理想来说, 因子链条件的情况如何. 确切地说, 我们将问, 如果因子链条件对于 $\mathfrak{R}$ 成立, 那么是否可以转移到 $\mathfrak{S}$ 中去, 根据 17.1 节的那些定理, 当对于 $\mathfrak{S}$ 来说已找出一个 $\mathfrak{R}$ 模基时, 这种转移是可能的. 这就是我们的第一个目的.

首先有一个预备定理:

定理　*设 σ 是 Σ 的一个元素, 那么 $\sigma=s/r$, 这里 $s\in\mathfrak{S}$, $r\in\mathfrak{R}$.*

证　元素 σ 满足一个系数属于 P 的方程. 这些系数是关于 $\mathfrak{R}$ 的分数. 乘以这些分母的乘积, 可以将这些系数化为 $\mathfrak{R}$ 中的量:

$$r_0\sigma^m+r_1\sigma^{m-1}+\cdots+r_m=0.$$

令 $r_0=r$, 并且乘以 r^{m-1}, 于是有

$$(r\sigma)^m+r_1(r\sigma)^{m-1}+r_2r(r\sigma)^{m-2}+\cdots+r_mr^{m-1}=0.$$

因此 $r\sigma$ 关于 $\mathfrak{R}$ 是整的. 令 $r\sigma=s$, 就得到这个断言.

由这个定理推出, Σ 是 $\mathfrak{S}$ 的商域.

定理　*如果元素 ξ 是整的, 那么 ξ 的一切共轭量 (在 Σ 的一个关于 P 的正规扩域内) 都是整的.*

证 根据假定, ξ 的一切幂都可以通过 Σ 中有限个量线性表示. 在 Σ 的一个同构之下, 这些量变成有限个量, 使得 ξ 的任一共轭量的一切幂都可以由这有限个量线性表示.

整量的和与积仍是整的, 因此, 在 ξ 共轭的量的初等对称函数也是整的. 由此推出:

定理 如果在一个整量 ξ 所满足的 P 上不可约方程里取最高系数等于 1, 那么其余的一切系数关于 $\mathfrak{R}$ 都是整的. 特别, 如果 $\mathfrak{R}$ 在 P 中是整闭的, 那么所有这些系数都属于 $\mathfrak{R}$.

在 $\mathfrak{R}$ 是整闭的情形下, 这个定理给了一个简便方法来考察一个量是不是整的: 我们无需作出 ξ 所满足的一切方程, 并且也无需检查在这些方程中是否存在一个整系数方程, 只要取一个最高系数是 1 的不可约方程即可. 如果这个不可约方程的一切系数都是整的, 那么 ξ 也是整的; 否则就不是.

我们现在作以下的约定:

(1) $\mathfrak{R}$ 在它的商域内是整闭的;

(2) 对 $\mathfrak{R}$ 中的理想因子链条件成立;

(3) Σ 是 P 的一个可分扩张.

根据 6.10 节, 由 (3) 推出, Σ 是由一个"本原元" σ 生成的: $\Sigma = P(\sigma)$. 根据上面的定理, $\sigma = s/r (s \in \mathfrak{S}, r \in \mathfrak{R})$. 从而整量 s 也生成这个域. s 满足一个 n 次方程, 此处 n 是域次数 (Σ/P). Σ 中每一元素 ξ 可以表示成

$$\xi = \sum_{0}^{n-1} \rho_k s^k \quad (\rho_k \in P) \tag{17.4}$$

的形状. 在 (17.4) 中将 s 代以它的共轭量 s_ν(在一个包含 Σ 的关于 P 的正规扩域内), 根据 6.8 节, 这样的共轭量正好有 n 个, 于是, 对于 ξ 的共轭量 ξ_ν, 我们得到方程组

$$\xi_\nu = \sum_{0}^{n-1} \rho_k s_\nu^k \quad (\nu = 1, 2, \cdots, n). \tag{17.5}$$

根据 Vandermonde 行列式定理, 这个方程组的行列式是

$$D = |s_\nu^k| = \prod_{\lambda < \mu} (s_\lambda - s_\mu).$$

它的平方是 s_ν 的一个对称函数从而属于 P. 再者, 因为共轭量 s_ν 都不相同, 所以 $D \neq 0$. 于是可以将方程组 (17.5) 解出

$$\rho_k = \frac{\sum S_{k\nu} \xi_\nu}{D},$$

此处 $S_{k\nu}$ 及 D 都是 s_ν 的多项式, 从而关于 $\mathfrak{R}$ 是整的. 把这些方程乘以 D^2, 于是得到

$$D^2\rho_k = \sum_\nu DS_{k\nu}\xi_\nu. \tag{17.6}$$

现在假定 ξ 是 $\mathfrak{S}$ 的元素, 因而是整的, 于是一切 ξ_ν 也都是整的, 从而 (17.6) 式右端是整的. 然而左端是 P 的一个元素. 根据 $\mathfrak{R}$ 在 P 中的整闭性, $D^2\rho_k$ 必须属于 $\mathfrak{R}$. 令 $D^2\rho_k = r_k$, 于是 $\rho_k = r_kD^{-2}$, 因此根据 (17.4),

$$\xi = \sum_0^{n-1} r_kD^{-2}s^k.$$

于是 $\mathfrak{S}$ 的每一元素 ξ 可以由 $D^{-2}s^0, D^{-2}s^1, \cdots, D^{-2}s^{n-1}$ 线性表示而系数取自 $\mathfrak{R}$. 换句话说, $\mathfrak{S}$ 被包含在有限 $\mathfrak{R}$ 模

$$\mathfrak{M} = (D^{-2}s^0, D^{-2}s^1, \cdots, D^{-2}s^{n-1})$$

内.

由此, 根据 17.1 节的定理得出, $\mathfrak{S}$ 连同 $\mathfrak{S}$ 的每一子模, 特别 $\mathfrak{S}$ 的每一理想, 都有一个关于 $\mathfrak{R}$ 的有限 $\mathfrak{R}$ 模基, 换句话说, 对于 $\mathfrak{S}$ 中的 $\mathfrak{R}$ 模, 特别对于 $\mathfrak{S}$ 中的理想来说, 因子链条件成立. 特别, 如果 $\mathfrak{R}$ 是一个主理想环, 那么 $\mathfrak{S}$ 以及 $\mathfrak{S}$ 的每一个子模都有一个线性无关的 $\mathfrak{R}$ 模基.

所谓在 Σ 中的一个 $\mathfrak{R}$序模指的是 Σ 的一个子环, 它包含 $\mathfrak{R}$ 并且是一个有限 $\mathfrak{R}$ 模. 根据上述, $\mathfrak{S}$ 是一个 $\mathfrak{R}$ 序模并且在 $\mathfrak{R}$ 与 $\mathfrak{S}$ 之间的每一环也是. 反过来, 由整性的定义立即得出, Σ 中每一个 $\mathfrak{R}$ 序模 $\mathfrak{T}$ 完全由整量所组成, 即包含在 $\mathfrak{S}$ 内. 由此我们可以将 $\mathfrak{S}$ 刻画为 Σ 中最大的 $\mathfrak{R}$ 序模. $\mathfrak{S}$ 也叫做域 Σ 的主序模. 于是, 当论及“域的理想”、“域的可逆元素”等等时, 我们永远理解作 $\mathfrak{S}$ 的理想, $\mathfrak{S}$ 的可逆元素等等. 根据 17.2 节, $\mathfrak{S}$ 在 Σ 中是整闭的.

这一节的结果对于 P 上的非交换代数来说不再成立, 这一事实所以失效, 主要在于两个整量的和不再是整量. 因此整量的全体不是序模. 尽管每一个序模完全由整量组成, 然而不存在一个包括一切序模的主序模. 在对于 Σ 的适当假设下, 存在不同的极大 $\mathfrak{R}$ 序模, 使得每一 $\mathfrak{R}$ 序模, 因而每一整元至少被包含在一个极大 $\mathfrak{R}$ 序模内. 关于这种极大 $\mathfrak{R}$ 序模的理想论可以看 Deuring M. Algebren. *Ergebn. Math. Bd.* 4, *Heft*, 1935, 1.

根据适才所证明的, 在 Σ 的一切 $\mathfrak{R}$ 序模内因子链条件成立. 因此对于这样的序模来说, 15.4 节及 15.5 节的分解定理及唯一性定理也成立 (将一切理想表作准素理想的交).

根据 15.8 节末, 当序模 $\mathfrak{o}$ 的每一个异于零理想的素理想都是极大理想时, 给理想论带来很大的简化. 以下定理指出在什么时候会出现这一情形：

定理　*如果在* $\mathfrak{R}$ *中每一* $\neq (0)$ *的素理想都是极大的, 那么在任意* $\mathfrak{R}$ *序模* $\mathfrak{o}$ *中, 每一* $\neq (0)$ *的素理想也是极大的.*

证　设 $\mathfrak{p}$ 是 $\mathfrak{o}$ 中一个素理想, 它含有一个非零元素 t, 它满足一个系数在 $\mathfrak{R}$ 内, 最高系数是 1 的最低次方程：

$$t^h + a_1 t^{h-1} + \cdots + a_h = 0,$$

其中必定 $a_h \neq 0$, 因为否则 t 可以从这整个方程中约去. 由此得 $a_h \equiv 0(t) \equiv 0(\mathfrak{p})$, 从而 a_h 属于交 $\mathfrak{p} \cap \mathfrak{R}$. 这个交是 $\mathfrak{R}$ 中一个素理想, 因为如果 $\mathfrak{R}$ 中两个元素的积属于 $\mathfrak{R} \cap \mathfrak{p}$, 从而属于 $\mathfrak{p}$, 那么必定有一个因子属于 $\mathfrak{p}$, 从而属于 $\mathfrak{R} \cap \mathfrak{p}$. 因为 a_h 属于素理想 $\mathfrak{R} \cap \mathfrak{p}$, 所以这个素理想不等于零理想, 从而是极大的.

现在设 $\mathfrak{a}$ 是 $\mathfrak{p}$ 的一个真因子, u 是 $\mathfrak{a}$ 中一个不属于 $\mathfrak{p}$ 的元素, 那么 u 仍然满足一个方程

$$u^l + b_1 u^{l-1} + \cdots + b_l = 0,$$

因而也满足一个最低次同余式

$$u^k + c_1 u^{k-1} + \cdots + c_k \equiv 0(\mathfrak{p}),$$

其中必定 $c_k \not\equiv 0(\mathfrak{p})$, 因为否则可以将 u 约去. 由此得 $c_k \equiv 0(u) \equiv 0(\mathfrak{a})$, 从而 c_k 属于交 $\mathfrak{a} \cap \mathfrak{R}$ 而不属于 $\mathfrak{p} \cap \mathfrak{R}$. 于是这个交 $\mathfrak{a} \cap \mathfrak{R}$ 是 $\mathfrak{p} \cap \mathfrak{R}$ 的一个真因子, 因而等于单位理想 $\mathfrak{R}$. 所以 $\mathfrak{a}$ 含有单位元, 从而 $\mathfrak{a} = \mathfrak{o}$, 证毕.

特别, 当 $\mathfrak{R}$ 是一个主理想环时 (整数环、域上一个不定元的多项式环), 这个定理的前提成立. 这时对于 $\mathfrak{o}$ 来说, 每一个异于零及单位的理想可以唯一地表示成异于 $\mathfrak{o}$ 的极大准素理想的积.

然而我们将看到, 对于主序模 $\mathfrak{S}$ 来说, 进一步还有：准素理想都是素理想的幂, 从而*每一理想都是素理想幂的积*. 对于古典的 Dedekind 理想论的这一主要结果, 由于它对于数域及函数域的理论的重要性, 我们将给出一个直接论证, 而不涉及准素理想的概念及一般理想论. 这一点将在下一节按照 Krull① 的一个方法来实现.

习题 17.4　设 $\mathfrak{R}$ 是一个主理想环, $(\omega_1, \cdots, \omega_n)$ 是一个序模 $\mathfrak{o}$ 的一组线性无关基 (在这一情形总存在一组线性无关基), 并且设 $(\omega_1^{(i)}, \cdots, \omega_n^{(i)})$ 是在 P 的一个正规扩域内的共轭基, 那么“域判别式”

$$D = \begin{vmatrix} \omega_1^{(1)} \cdots \omega_n^{(1)} \\ \vdots \qquad \vdots \\ \omega_1^{(n)} \cdots \omega_n^{(n)} \end{vmatrix}^2$$

① Krull W. Zur theorie der allgemeinen zahlring. *Math. Ann.*, 1928, 99: 51–70.

是整、有理的且异于零.

习题 17.5　设 $\Sigma = P(\sqrt{d})$ 而 $\mathfrak{R}$ 在 P 中整闭. 证明, 数 $\xi = a + b\sqrt{d}$ 关于 $\mathfrak{R}$ 是整的, 当且仅当迹与范数:

$$S(\xi) = \xi + \xi' = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a,$$
$$N(\xi) = \xi \cdot \xi' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$$

都属于$\mathfrak{R}$.

习题 17.6　在习题 17.5 里, 如果 $\mathfrak{R} = K[x]$ 是一个不定元的多项式环而 d 是一个没有重因子的多项式, 那么 $\xi = a + b\sqrt{d}$ 是整的, 仅当 a 与 b 都属于 $\mathfrak{R}$.

习题 17.7　在习题 17.5 里, 如果 $\mathfrak{R} = \mathbb{Z}$ 是整数环而 d 是一个无平方因子的整数, 那么当 $d \not\equiv 1(4)$ 时, 数 1, $\sqrt{d}$ 组成主序模的一个基; 当 $d \equiv 1(4)$ 时, 数 1, $\dfrac{1+\sqrt{d}}{2}$ 组成主序模的一个基.

17.4　古典理想论的公理根据

设 $\mathfrak{o}$ 是一个整环 (无零因子的交换环), 在其中下列三个公理被满足:

I. 对理想的因子链条件;

II. 一切异于零理想的素理想都是极大的;

III. $\mathfrak{o}$在商域 Σ 内是整闭的.

这样的环的例子是: (1) 主理想环; (2) 在商域的有限扩张下按 17.3 节的图式由主理想环所产生的主序模 (特别是数域及一个变量的函数域中的主序模).

根据 III, Σ 中关于 $\mathfrak{o}$ 的整元属于 $\mathfrak{o}$, 并且将简称作整元素. 特别, Σ 的单位元素总是整的, 从而 $\mathfrak{o}$ 是一个有单位元的整环.

现在除了 $\mathfrak{o}$ 的理想 (或 $\mathfrak{o}$ 中的 $\mathfrak{o}$ 模) 外, 我们还考虑 Σ 中的 $\mathfrak{o}$模, 就是 Σ 的子集, 它在含有 a 与 b 的同时也含有 $a-b$, 并且在含有 a 的同时也含有 ra(此处 r 是整的). 如果一个这样的 $\mathfrak{o}$ 模有一个有限模基, 那么也称它为分式理想. 如果一个 $\mathfrak{o}$ 模 $\mathfrak{a}$ 完全由整量组成 ($\mathfrak{a} \subseteq \mathfrak{o}$), 因而它是一个在通常意义下的理想, 或者如我们现在所说的, 一个整理想.

两个 $\mathfrak{o}$ 模 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的和或最大公因子指的是 (正如在理想的情形一样) 一切和 $a+b$ 所组成的模, 其中 $a \in \mathfrak{a}, b \in \mathfrak{b}$. 同样, 积 $\mathfrak{ab}$ 指的是由一切积 ab 所生成的模, 即一切和 $\sum a_\nu b_\nu$ 的全体.

具有限模基的 $\mathfrak{o}$ 模的和与积仍具有限模基.

在以下的定理里, 德文字母专门用来表示 $\mathfrak{o}$ 中的异于零理想的整理想, 同时字母 $\mathfrak{p}$ 总表示一个 $\neq (0)$ 的素理想.

引理 1　对于每一个理想 $\mathfrak{a}$, 存在一组素理想 $\mathfrak{p}_i$, 其中每一个 $\mathfrak{p}_i$ 都是 $\mathfrak{a}$ 的因

子, 而它们的积可以被 $\mathfrak{a}$ 整除:

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r\equiv 0(\mathfrak{a}).$$

证 如果 $\mathfrak{a}$ 是素理想, 那么引理成立. 设 $\mathfrak{a}$ 不是素理想, 那么存在两个主理想 $\mathfrak{b}$, $\mathfrak{c}$, 使得

$$\mathfrak{b}\mathfrak{c}\equiv 0(\mathfrak{a}),\quad \mathfrak{b}\not\equiv 0(\mathfrak{a}),\quad \mathfrak{c}\not\equiv 0(\mathfrak{a}).$$

理想 $\mathfrak{b}'=(\mathfrak{b},\mathfrak{a}),\mathfrak{c}'=(\mathfrak{c},\mathfrak{a})$ 是 $\mathfrak{a}$ 的真因子, 并且

$$\mathfrak{b}'\mathfrak{c}'=(\mathfrak{b},\mathfrak{a})\cdot(\mathfrak{c},\mathfrak{a})=(\mathfrak{b}\mathfrak{c},\mathfrak{b}\mathfrak{a},\mathfrak{a}\mathfrak{c},\mathfrak{a}^2)\equiv 0(\mathfrak{a},\mathfrak{a},\mathfrak{a})\equiv 0(\mathfrak{a}).$$

现在假设定理对于理想 $\mathfrak{b}'$ 与 $\mathfrak{c}'$ 成立, 那么存在一个积 $\mathfrak{p}_1\cdots\mathfrak{p}_s\equiv 0(\mathfrak{b}')$ 及另一个积 $\mathfrak{p}_{s+1}\cdots\mathfrak{p}_r\equiv 0(\mathfrak{c}')$. 于是乘积 $\mathfrak{p}_1\cdots\mathfrak{p}_s\mathfrak{p}_{s+1}\cdots\mathfrak{p}_r\equiv 0(\mathfrak{b}'\cdot\mathfrak{c}')\equiv 0(\mathfrak{a})$, 从而定理也对 $\mathfrak{a}$ 成立. 因此, 如果定理对于某一理想 $\mathfrak{a}$ 不成立, 那么它将对于 $\mathfrak{a}$ 的两个真因子之一 $\mathfrak{b}'$ 或 $\mathfrak{c}'$ 也不成立. 同样, 又后者有一个真因子, 对它来说定理不成立, 如此等等. 于是就得到一个真因子的无限链, 根据公理 I 这是不可能的. 因此定理对于每一理想 $\mathfrak{a}$ 成立.

引理 2 *若 $\mathfrak{p}$ 是素理想, 那么由 $\mathfrak{a}\mathfrak{b}\equiv 0(\mathfrak{p})$ 得出 $\mathfrak{a}\equiv 0(\mathfrak{p})$ 或 $\mathfrak{b}\equiv 0(\mathfrak{p})$.*

证 如果 $\mathfrak{a}\not\equiv 0(\mathfrak{p})$ 且 $\mathfrak{b}\not\equiv 0(\mathfrak{p})$, 那么存在 $\mathfrak{a}$ 的一个元素 a 及 $\mathfrak{b}$ 的一个元素 b, 它们都不属于 $\mathfrak{p}$. 乘积 ab 属于 $\mathfrak{a}\mathfrak{b}$, 从而属于 $\mathfrak{p}$, 这与 $\mathfrak{p}$ 的素理想性质相违.

我们用 $\mathfrak{p}^{-1}$ 表示 (整或分式) 量 a 的全体, 对于这样的 a, $a\mathfrak{p}$ 是整的. $\mathfrak{p}^{-1}$ 显然是一个 $\mathfrak{o}$ 模.

引理 3 *若 $\mathfrak{p}\neq\mathfrak{o}$, 那么在 $\mathfrak{p}^{-1}$ 中有一个非整元素.*

证 设 c 是 $\mathfrak{p}$ 中任意一个异于零的元素. 根据引理 1, 存在一个素理想积

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r\equiv 0(c).$$

我们可以假定这个积是不可缩短的, 即没有任何部分积, 例如 $\mathfrak{p}_2\cdots\mathfrak{p}_r\equiv 0(c)$. 因为积 $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$ 可以被 $\mathfrak{p}$ 整除, 所以必定有一个因子, 例如 $\mathfrak{p}_1$, 可以被 $\mathfrak{p}$ 整除, 从而等于 $\mathfrak{p}$.

于是

$$\mathfrak{p}\mathfrak{p}_2\cdots\mathfrak{p}_r\equiv 0(c),$$
$$\mathfrak{p}_2\cdots\mathfrak{p}_r\not\equiv 0(c).$$

因此在 $\mathfrak{p}_2\cdots\mathfrak{p}_r$ 内存在一个不属于 (c) 的元素 b. 对于这个元素, 有

$$\mathfrak{p}b\equiv 0(\mathfrak{p}\mathfrak{p}_2\cdots\mathfrak{p}_r)\equiv 0(c).$$

因此 $\mathfrak{p}b/c$ 是整的. 从而 b/c 属于 $\mathfrak{p}^{-1}$. 然而由于 $b\not\equiv 0(c)$, 所以 b/c 不是整的, 证毕.

定理 1 若$\mathfrak{p} \neq \mathfrak{o}$, 那么

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{o}.$$

证 根据 $\mathfrak{p}^{-1}$ 的定义, $\mathfrak{o} \subseteq \mathfrak{p}^{-1}$, 从而 $\mathfrak{p} = \mathfrak{o}\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}$. 因此整理想 $\mathfrak{p}\mathfrak{p}^{-1}$ 是 $\mathfrak{p}$ 的因子, 从而或者 $= \mathfrak{p}$ 或者 $= \mathfrak{o}$. 假定

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}.$$

由此将推出：$\mathfrak{p} \cdot (\mathfrak{p}^{-1})^2 = (\mathfrak{p} \cdot \mathfrak{p}^{-1})\mathfrak{p}^{-1} = \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. 同样 $\mathfrak{p}(\mathfrak{p}^{-1})^3 = \mathfrak{p}$, 等等. 于是, 若 $a \neq 0$ 是 $\mathfrak{p}$ 的任意一个元素而 b 是 $\mathfrak{p}^{-1}$ 的一个元素, 那么 $ab^e \in \mathfrak{p}(\mathfrak{p}^{-1})^e$ 是整的, 从而 b 的一切幂都可以表示成具有一个固定分母的分数. 所以 b 是整的. 这对 $\mathfrak{p}^{-1}$ 的每一元素 b 都成立, 与引理 3 矛盾.

我们现在可以证明关于因子分解的主要定理：

定理 2 每一理想 $\mathfrak{a}$ 都是素理想的积.

证 我们可以假定 $\mathfrak{a} \neq \mathfrak{o}$. 根据引理 1, 设

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \equiv 0(\mathfrak{a}), \tag{17.7}$$

并且数 r 选得尽可能地小, 使得没有更短的乘积 $\equiv 0(\mathfrak{a})$. 仍设 $\mathfrak{p}$ 是 $\mathfrak{a}$ 的任意一个异于 $\mathfrak{o}$ 的素理想因子 (根据引理 1, 这样一个因子必定存在). 于是乘积 $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ 可以被 $\mathfrak{p}$ 整除, 从而 (根据引理 2) 有一个 $\mathfrak{p}_i$ 可以被 $\mathfrak{p}$ 整除. 因为这个 $\mathfrak{p}_i$ 是极大的, 所以 $\mathfrak{p}_i = \mathfrak{p}$. 不妨假定 $\mathfrak{p}_1 = \mathfrak{p}$. 以 $\mathfrak{p}^{-1}$ 乘 (17.7) 式, 于是有

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \equiv 0(\mathfrak{p}^{-1}\mathfrak{a}) \equiv 0(\mathfrak{o}).$$

因此 $\mathfrak{p}^{-1}\mathfrak{a}$ 是一个整理想, 它已经能够整除一个少于 r 个 $\neq (0)$ 的素理想的乘积. 现在对 r 进行归纳, 即假定对于能够整除少于 r 个素理想的积的那样的理想来说, 定理已被证明 (对于能整除一个 $\neq (0)$ 的理想来说是显然的), 那么定理特别对于 $\mathfrak{p}^{-1}\mathfrak{a}$ 成立. 即

$$\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}_2' \cdots \mathfrak{p}_s'.$$

两端同乘以 $\mathfrak{p}$ 就得到所寻求的 $\mathfrak{a}$ 的表示.

这种表示的唯一性由以下定理推出.

定理 3 如果 $\mathfrak{a} \equiv 0(\mathfrak{b})$ 且 $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathfrak{b} = \mathfrak{p}_1' \cdots \mathfrak{p}_s'$, 那么在 $\mathfrak{b}$ 的表示中出现的每一个异于 $\mathfrak{o}$ 的素理想也在$\mathfrak{a}$的表示中出现, 并且至少以同样多次出现.

证 设 $\mathfrak{p}_1' \neq \mathfrak{o}$. 因为 $\mathfrak{p}_1'$ 是 $\mathfrak{a}$ 的因子, 所以如上所述, $\mathfrak{p}_1'$ 必定在 $\mathfrak{p}_\nu$ 中出现. 例如设 $\mathfrak{p}_1 = \mathfrak{p}_1'$. 于是有

$$\mathfrak{p}_1^{-1}\mathfrak{a} \equiv 0(\mathfrak{p}_1^{-1}\mathfrak{b}),$$
$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_2 \cdots \mathfrak{p}_r,$$
$$\mathfrak{p}_1^{-1}\mathfrak{b} = \mathfrak{p}_2' \cdots \mathfrak{p}_s'.$$

我们假设定理对于 s 的较小的值已经证明 (对于 $s=0$, $\mathfrak{b}=\mathfrak{o}$ 来说是自明的), 于是推出, 每一个异于 $\mathfrak{o}$ 的理想 $\mathfrak{p}_2',\cdots,\mathfrak{p}_s'$ 至少以同样多次出现在 $\mathfrak{p}_2,\cdots,\mathfrak{p}_r$ 中, 从而断言得到证明.

推论 1 理想 $\mathfrak{a}$ 被表成素理想积的表示中, 除因子的次序及因子 $\mathfrak{o}$ 外是唯一的.

推论 2 由整除性可以得出乘积表示：如果 $\mathfrak{a}\equiv 0(\mathfrak{b})$, 那么 $\mathfrak{a}=\mathfrak{b}\mathfrak{c}$, 其中 $\mathfrak{c}$是整的.

我们只需取 $\mathfrak{a}$ 的这样的素因子的积作为 $\mathfrak{c}$, 即从 $\mathfrak{a}$ 的表示式中去掉 $\mathfrak{b}$ 中的素因子 (每一个的次数与它在 $\mathfrak{b}$ 中出现的次数相同) 所剩下的乘积.

习题 17.8 在数域 $\mathbb{Q}(\sqrt{-5})$ 的主序模中, 分解主理想 (2) 与 (3) 为素理想因子.

17.5 上节结果的逆及其推论

我们已经看到, 定理 2 与定理 3(17.4 节) 由公理 I~III 得出, 这两个定理合并起来说的就是理想的唯一素因子分解. 现在这一事实的反面也是成立的.

设 $\mathfrak{o}$ 是一个有单位元的整环. 又设在 $\mathfrak{o}$ 中每一整理想 $\mathfrak{a}$ 都能表示成素理想的积：$\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$, 并且如果 $\mathfrak{a}$ 能被 $\mathfrak{b}$ 整除, 那么在 $\mathfrak{a}$ 的任一分解中每一个异于 $\mathfrak{o}$ 的因子出现的次数至少与它在 $\mathfrak{b}$ 的分解中出现的次数一样多. 于是在 $\mathfrak{o}$ 中公理 I~III 成立.

证 因为每一个整理想 $\mathfrak{a}=\mathfrak{p}_1^{\rho_1}\cdots\mathfrak{p}_r^{\rho_r}$ 只有有限多个因子 $\mathfrak{b}=\mathfrak{p}_1^{\sigma_1}\cdots\mathfrak{p}_r^{\sigma_r}(\sigma_i\leqslant\rho_i)$, 从而立即得出因子链条件 (公理 I). 特别, 一个素理想 $\mathfrak{p}$ 只有因子 $\mathfrak{p}$ 及 $\mathfrak{o}$, 因此公理 II 也成立.

为了证明公理 III ($\mathfrak{o}$ 在商域 Σ 中的整闭性), 设 λ 是 Σ 的一个元素, 它对于 $\mathfrak{o}$ 是整的, 从而例如 λ^m 可以由 $\lambda^0,\cdots,\lambda^{m-1}$ 线性表示, 或者换一句话说, λ^m 属于 $\mathfrak{o}$ 模 $\mathfrak{l}=(\lambda^0,\lambda^1,\cdots,\lambda^{m-1})$. 若 $\lambda=a/b$, 那么将 $\mathfrak{l}$ 乘以 $\mathfrak{b}=(b^{m-1})$ 可以变为一个整理想. 再者, $\mathfrak{l}$ 显然满足方程 $\mathfrak{l}^2=\mathfrak{l}$. 用 $\mathfrak{b}^2$ 乘, 得到

$$(\mathfrak{l}\mathfrak{b})^2=(\mathfrak{l}\mathfrak{b})\mathfrak{b}.$$

于是由唯一性推出

$$\mathfrak{l}\mathfrak{b}=\mathfrak{b},$$

由此, 当两端再乘以 $b^{-(m-1)}$ 时, 就得到

$$\mathfrak{l}=\mathfrak{o}.$$

因而 λ 是 $\mathfrak{o}$ 的元素, 证毕.

我们现在将考虑定理 2 及定理 3 的某些推论, 它们同样也是属于古典的理想论的.

由整除性推出乘积表示这一事实, 使得我们可以按照如同在整数的情形利用素因子分解的方法那样来计算理想的最大公因子及最小公倍.

设 $\mathfrak{a}$ 与 $\mathfrak{b}$ 是两个整理想：

$$\begin{aligned}\mathfrak{a}&=\mathfrak{p}_1^{\rho_1}\cdots\mathfrak{p}_r^{\rho_r},\\ \mathfrak{b}&=\mathfrak{p}_1^{\sigma_1}\cdots\mathfrak{p}_r^{\sigma_r}\end{aligned}$$

(在这两个等式里, 将出现在 $\mathfrak{a}$ 与 $\mathfrak{b}$ 中的一切素因子完全写出, 可能带有指数零). 每一个公因子只含有出现在这个序列里的素因子 $\mathfrak{p}_i$ 并且带有指数 $\leqslant\tau_i$, 此处 τ_i 是数 ρ_i, σ_i 中较小的一个. 最大公因子 $(\mathfrak{a},\mathfrak{b})$ 必定能被每一公因子, 特别能被 $\mathfrak{p}_i^{\tau_i}$ 整除. 于是它只能是

$$\mathfrak{p}_1^{\tau_1}\cdots\mathfrak{p}_r^{\tau_r}.$$

同样, $\mathfrak{a}$ 与 $\mathfrak{b}$ 的最小公倍 (交) $\mathfrak{a}\cap\mathfrak{b}$ 是理想

$$\mathfrak{p}_1^{\mu_1}\cdots\mathfrak{p}_r^{\mu_r},$$

此处 μ_i 是数 ρ_i, σ_i 中较大的一个.

定理 4　如果 $\mathfrak{a}\equiv 0(\mathfrak{d})$, 那么在 $\mathfrak{d}$ 内存在一个元素 d, 使得

$$(\mathfrak{a},d)=\mathfrak{d}.$$

证　设

$$\begin{aligned}\mathfrak{a}&=\mathfrak{p}_1^{\rho_1}\cdots\mathfrak{p}_r^{\rho_r},\\ \mathfrak{b}&=\mathfrak{p}_1^{\sigma_1}\cdots\mathfrak{p}_r^{\sigma_r}\quad(0\leqslant\sigma_i\leqslant\rho_i).\end{aligned}$$

我们需要如此选择 d, 使得 d 能被 $\mathfrak{d}$ 整除, 但是除 $\mathfrak{d}$ 的因子外与 $\mathfrak{a}$ 不再有任何公因子. 令

$$\begin{aligned}\mathfrak{c}&=\mathfrak{p}_1^{\sigma_1+1}\cdots\mathfrak{p}_r^{\sigma_r+1},\\ \mathfrak{c}_i&=\mathfrak{c}:\mathfrak{p}_i=\mathfrak{p}_1^{\sigma_1+1}\cdots\mathfrak{p}_i^{\sigma_i}\cdots\mathfrak{p}_r^{\sigma_r+1}.\end{aligned}$$

那么 $\mathfrak{c}_i\not\equiv 0(\mathfrak{c})$. 因此存在一个元素 d_i, 它属于 $\mathfrak{c}_i$ 但不属于 $\mathfrak{c}$. 于是

$$\begin{aligned}&d_i\equiv 0(\mathfrak{p}_j^{\sigma_j+1}),\quad \text{对于} j\neq i,\\ &d_i\not\equiv 0(\mathfrak{p}_i^{\sigma_i+1})\end{aligned}$$

和

$$d=d_1+\cdots+d_r$$

可以被 $\mathfrak{d}$ 整除 (因为一切 d_i 都能被 $\mathfrak{d}$ 整除). 然而

$$d \equiv d_i \not\equiv 0(\mathfrak{p}_i^{\sigma_i+1}).$$

因此 d 与 $\mathfrak{a}$ 除 $\mathfrak{d}$ 的因子外, 的确不再有任何公因子.

推论 1　在同余类环 $\mathfrak{o}/\mathfrak{a}$ 内每一理想 $\mathfrak{d}/\mathfrak{a}$ 都是主理想. $\mathfrak{d}/\mathfrak{a}$ 由同余类 $\mathfrak{a}+d$ 生成.

推论 2　每一理想 $\mathfrak{d}$ 都有一个二项基 (a, d), 此处 $a \neq 0$ 可以在 $\mathfrak{d}$ 中任意选取.

即令 a 是 $\mathfrak{d}$ 中任意非零元素, 且 $\mathfrak{a}=(a)$. 由以上定理得 $(a, d)=\mathfrak{d}$.

推论 3　每一理想 $\mathfrak{d}$ 都可以通过乘以一个与给定的理想 $\mathfrak{c}$ 无公因子的理想 $\mathfrak{b}$ 而化为一个主理想.

证　令 $\mathfrak{a}=\mathfrak{c}\mathfrak{d}$. 由以上定理得

$$(\mathfrak{a}, d)=\mathfrak{d}. \tag{17.8}$$

因为 d 可以被 $\mathfrak{d}$ 整除, 所以可以令

$$(d)=\mathfrak{b}\mathfrak{d}.$$

于是由 (17.8) 得

$$(\mathfrak{c}\mathfrak{d}, \mathfrak{b}\mathfrak{d})=\mathfrak{d}.$$

从而 $\mathfrak{c}$ 与 $\mathfrak{b}$ 必定无公因子.

习题 17.9　令 $\mathfrak{O}$ 是一切商 a/b 的环, 此处 a, b 是整的而 b 不能被给定的素理想 $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ 整除. 那么对于 $\mathfrak{o}$ 的每一个理想 $\mathfrak{a}$ 有 $\mathfrak{O}$ 的一个理想 $\mathfrak{A}$ 与它对应, $\mathfrak{A}$ 由分式 a/b 组成, $a \in \mathfrak{a}$. 对于素理想 $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ 有素理想 $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ 与它们对应, $\mathfrak{o}$ 的其余的一切素理想对应着 $\mathfrak{O}$ 的单位理想. $\mathfrak{O}$ 的每一个理想可以唯一地表示成理想 $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ 的幂积. 再者, $\mathfrak{O}$ 的每一理想都是主理想.

17.6　分 式 理 想

在 17.4 节我们称商域 Σ 中一个具有有限基的 $\mathfrak{o}$ 模为分式理想. 因此 $\mathfrak{o}$ 的理想, 或“整理想”是特殊的分式理想.

如果 $(\sigma_1, \cdots, \sigma_r)$ 是一个分式理想的一个基, 那么通过乘以一个适当的分母, 可以将整个的基, 从而将这个理想本身化为整的.

反过来, 如果一个 $\mathfrak{o}$ 模 $\mathfrak{a}$ 可以通过乘以一个整量 $b \neq 0$ 化为整理想, 那么作为整理想, $b\mathfrak{a}$ 有一个有限基

$$b\mathfrak{a}=(a_1, \cdots, a_r),$$

由此得

$$\mathfrak{a}=\left(\frac{a_1}{b},\cdots,\frac{a_r}{b}\right).$$

这样就证明了：

定理 Σ 的一个 $\mathfrak{o}$ 模是一个分式理想, 当且仅当它可以通过乘以一个整量 $b\neq 0$ 化为一个整理想.

我们已经看到, 如果 $\mathfrak{a}$ 与 $\mathfrak{b}$ 都有有限基, 那么 $\mathfrak{a}\cdot\mathfrak{b}$ 及 $(\mathfrak{a},\mathfrak{b})$ 也有有限基, 从而也是分式理想. 同一结论对于模商 $\mathfrak{a}:\mathfrak{b}$ 也成立, 此处 $\mathfrak{a}$ 与 $\mathfrak{b}$ 都是整理想且 $\mathfrak{b}\neq(0)$[①]. 这因为, 如果 $b\neq 0$ 是 $\mathfrak{b}$ 的任意一个元素, 那么

$$b\cdot(\mathfrak{a}:\mathfrak{b})\subseteq\mathfrak{b}\cdot(\mathfrak{a}:\mathfrak{b})\subseteq\mathfrak{a}\subseteq\mathfrak{o}.$$

从而 $\mathfrak{a}:\mathfrak{b}$ 通过乘以 b 化为一个整理想.

特别, $\mathfrak{o}:\mathfrak{p}=\mathfrak{p}^{-1}$ 总是一个分式理想.

每一个 $\neq(0)$ 的整理想或分式理想都有一个逆.

证 设 $\mathfrak{c}$ 是一个 $\neq(0)$ 的整理想或分式理想, 且如此选取 $b\neq 0$, 使得 $b\mathfrak{c}$ 是整的：

$$b\mathfrak{c}=\mathfrak{a}. \tag{17.9}$$

现在设 $\mathfrak{a}=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$, 那么根据定理 1(17.4 节), 将 (17.9) 乘以 $\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}\cdots\mathfrak{p}_r^{-1}$, 得到

$$(\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}\cdots\mathfrak{p}_r^{-1}b)\mathfrak{c}=\mathfrak{o},$$

从而证明了逆

$$\mathfrak{c}^{-1}=\mathfrak{p}_1^{-1}\cdots\mathfrak{p}_r^{-1}b$$

存在.

由这个定理推出：$\neq(0)$ 的整理想与分式理想作成一个 Abel 群.

于是方程 $\mathfrak{a}\mathfrak{c}=\mathfrak{b}$ 对 $\mathfrak{c}$ 唯一可解. 这个解可以记作 $\mathfrak{a}^{-1}\mathfrak{b}$ 或 $\mathfrak{b}/\mathfrak{a}$.

由以上定理还推出：

每一个分式理想作为两个整理想的商：

$$\frac{\mathfrak{p}_1'\cdots\mathfrak{p}_s'}{\mathfrak{p}_1''\cdots\mathfrak{p}_t''}.$$

在这个表示式里可以将同时出现在分子及分母中的理想约去.

每一个分式主理想 (λ) 可以表示成两个整主理想的商, 具有以下性质：使得任意给定的 r 个素理想中没有一个既在分子又在分母中出现.

---

① 关于模商 $\mathfrak{a}:\mathfrak{b}$(在 Σ 内) 我们理解为 Σ 中满足 $\lambda\mathfrak{b}\subseteq\mathfrak{a}$ 的元素 λ 的全体.

证　设已经约简的表示为

$$(\lambda)=\frac{\mathfrak{p}_1'\cdots\mathfrak{p}_s'}{\mathfrak{p}_1''\cdots\mathfrak{p}_t''},$$

并且设 $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ 是 r 个给定的素理想. 通过乘以一个与乘积 $\mathfrak{p}_1\cdots\mathfrak{p}_r$ 无公因子的理想 $\mathfrak{b}$ 将分母化为一个主理想 (d), 那么

$$(\lambda)=\frac{\mathfrak{b}\mathfrak{p}_1'\cdots\mathfrak{p}_s'}{\mathfrak{b}\mathfrak{p}_1''\cdots\mathfrak{p}_t''}=\frac{\mathfrak{b}\mathfrak{p}_1'\cdots\mathfrak{p}_s'}{(d)},$$

于是

$$\mathfrak{b}\mathfrak{p}_1'\cdots\mathfrak{p}_s'=(\lambda d).$$

这个分子同样也是主理想. 理想 $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ 中没有一个既在分子又在分母中出现.

习题 17.10　理想分式 $\mathfrak{a}^{-1}\mathfrak{b}$ 等于模商 $\mathfrak{b}:\mathfrak{a}$[①].

17.7　任意整闭整环中的理想论

有许多重要的整环, 它们虽然满足 17.4 节的公理 I 及 III, 然而却不满足公理 II. 我们只提出多于一个变量的多项式环 $K[x_1,\cdots,x_n]$, 整系数多项式环 $\mathbb{Z}[x_1,\cdots,x_n]$ 以及它们的有限整闭扩张 (主序模) 作为例子. 在所有这些环里, 一个异于零及单位理想的素理想可能有一个同样也异于零及单位理想的素理想作为真因子. 因此在这样的环里, 17.4 节的理想论不成立. 然而我们将指出, 如果将理想的相等用一个即将定义的“拟相等”关系来代替, 其中的主要结果仍旧保持[②].

设 $\mathfrak{o}$ 是一个整环, 在它的商域 Σ 内是整闭的. 以下用德文字母表示异于零理想的分式理想, 即 Σ 中的 $\mathfrak{o}$ 模, 它可以通过用 $\mathfrak{o}$ 中一个异于零的元素去乘而变为整的. 关于逆理想 $\mathfrak{a}^{-1}$ 仍指的是 Σ 中这样的元素 r 的全体, 对于这样的元素来说, $r\mathfrak{a}$ 是整的.

定义. $\mathfrak{a}$ 拟相等于 $\mathfrak{b}$, 如果 $\mathfrak{a}^{-1}=\mathfrak{b}^{-1}$. 记作 $\mathfrak{a}\sim\mathfrak{b}$. 关系 $\sim$ 显然是自反的、对称的和传递的.

同样, $\mathfrak{a}$ 叫做 $\mathfrak{b}$ 的一个拟因子, $\mathfrak{b}$ 叫做 $\mathfrak{a}$ 的一个拟倍, 如果 $\mathfrak{a}^{-1}\subseteq\mathfrak{b}^{-1}$, 换句话说, 如果 $\mathfrak{a}^{-1}\mathfrak{b}$ 是整的. 记作 $\mathfrak{a}\leqslant\mathfrak{b}$ 或 $\mathfrak{b}\geqslant\mathfrak{a}$.

符号 $\leqslant$ 及 $\sim$ 的简单性质是:

---

① 关于数域中理想论的进一步发展可以参考 Hecke E. Vorlesungen über die Theorie der Algebraischen Zahlen. *Leipzig*, 1923. 关于函数域中的理想论和它的应用可参考 Dedekind 及 Weber 的奠基性著作：Crelles Journal, 1882, 92：181.

② 由作者在*Math. Ann.*, 1929, 101 所建立的理论由 Artin 修改为比较完美的形式, 并且以这个形式在这里首次发表.

(1) 由 $\mathfrak{a} \supseteq \mathfrak{b}$ 得 $\mathfrak{a} \leqslant \mathfrak{b}$(证明显然).

(2) 如果 $\mathfrak{a}$ 是主理想：$\mathfrak{a} = (a)$, 那么由 $\mathfrak{a} \leqslant \mathfrak{b}$ 反过来便得出 $\mathfrak{a} \supseteq \mathfrak{b}$. 因为这时 $\mathfrak{a}^{-1} = (a^{-1})$. 根据假设, $\mathfrak{a}^{-1}\mathfrak{b}$ 是整的, 于是 $a^{-1}\mathfrak{b}$ 是整的, 这就是说, $\mathfrak{b}$ 的一切元素可以被 a 整除.

(3) $\mathfrak{a} \leqslant \mathfrak{b}$ 且同时 $\mathfrak{a} \geqslant \mathfrak{b}$, 那么 $\mathfrak{a} \sim \mathfrak{b}$.

(4) $\mathfrak{a}$ 的一切拟倍 $\mathfrak{b}$, 特别, 一切与 $\mathfrak{a}$ 拟相等的 $\mathfrak{b}$, 具有性质 $\mathfrak{b} \subseteq (\mathfrak{a}^{-1})^{-1}$(由 $\mathfrak{b}\mathfrak{a}^{-1}$ 的整性立刻得出).

因此, 特别有 $\mathfrak{a} \subseteq (\mathfrak{a}^{-1})^{-1}$. 由此根据 (1) 得 $\mathfrak{a} \geqslant (\mathfrak{a}^{-1})^{-1}$. 另一方面, $\mathfrak{a}^{-1}(\mathfrak{a}^{-1})^{-1}$ 是整的, 从而 $\mathfrak{a} \leqslant (\mathfrak{a}^{-1})^{-1}$, 于是

$$\mathfrak{a} \sim (\mathfrak{a}^{-1})^{-1}. \tag{5}$$

根据 (4) 与 (5), $(\mathfrak{a}^{-1})^{-1}$ 是与 $\mathfrak{a}$ 拟相等的最大理想. 将它记作 $\mathfrak{a}^*$.

(6) 如果 $\mathfrak{a} \leqslant \mathfrak{b}$, 那么 $\mathfrak{a}\mathfrak{c} \leqslant \mathfrak{b}\mathfrak{c}$. 因为 $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c}\mathfrak{a}$ 是整的, 所以 $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c} \subseteq \mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$, 从而 $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c}\mathfrak{b}$ 是整的, 或 $\mathfrak{c}\mathfrak{a} \leqslant \mathfrak{c}\mathfrak{b}$.

(7) 如果 $\mathfrak{a} \sim \mathfrak{b}$, 那么 $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c}$ (由 (6) 得出).

(8) 如果 $\mathfrak{a} \sim \mathfrak{b}$ 且 $\mathfrak{c} \sim \mathfrak{d}$, 那么 $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$(因为由 (7)$\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$).

如果将与一个理想拟相等的一切理想归并成一类, 那么根据 (8), 乘积 $\mathfrak{a}\mathfrak{c}$ 的类仅与 $\mathfrak{a}$ 的类及 $\mathfrak{c}$ 的类有关. 因此我们可以定义后两类的乘积为乘积 $\mathfrak{a}\mathfrak{c}$ 的类.

(9) 关于类的乘法的单位类是与单位理想 $\mathfrak{o}$ 拟相等的理想所在的类. 因为对于每一理想 $\mathfrak{a}$ 来说, $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$.

(10) $\mathfrak{o}$ 的一切拟倍, 特别是单位类中的一切理想, 都是整的 ((2) 的特殊情形：令 $a = 1$). 由此推出, 与一个整理想拟相等的一切理想仍是整的.

我们现在证明关于逆理想的最重要的性质：

$$\mathfrak{a}\mathfrak{a}^{-1} \sim \mathfrak{o}. \tag{11}$$

$\mathfrak{a}\mathfrak{a}^{-1} \geqslant \mathfrak{o}$ 是显然的, 因为 $\mathfrak{a}\mathfrak{a}^{-1}$ 是整的. 只剩下证明 $\mathfrak{a}\mathfrak{a}^{-1} \leqslant \mathfrak{o}$, 或 $(\mathfrak{a}\mathfrak{a}^{-1})^{-1} \subseteq \mathfrak{o}$. 如果 λ 属于 $(\mathfrak{a}\mathfrak{a}^{-1})^{-1}$, 那么 $\lambda\mathfrak{a}\mathfrak{a}^{-1}$ 是整的, 因此 $\lambda\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$, $\lambda^2\mathfrak{a}^{-1} \subseteq \lambda\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$, 等等, 一般 $\lambda^n\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$, 从而$\lambda^n\mathfrak{a}^{-1}\mathfrak{a}$ 是整的. 如果 μ 是 $\mathfrak{a}^{-1}\mathfrak{a}$ 的任意一个元素, 那么 λ 的一切幂乘以 μ 以后是整的. 由 $\mathfrak{o}$ 的整闭性, 正如 17.4 节中定理 1 的证明那样, 推出 λ 本身是整的.

由 (11) 推出, 在上面所定义的类的乘法之下, $\mathfrak{a}^{-1}$ 的类是 $\mathfrak{a}$ 的类的逆：$\mathfrak{a}$ 的类与 $\mathfrak{a}^{-1}$ 的类的积是单位类. 于是

定理 1 *拟相等理想类作成一个群.*

以下两个规则使我们可以将拟整除性及拟相等性除去单位类的因子外分别作为整除性及相等性来刻画：

(12) 由 $\mathfrak{a} \geqslant \mathfrak{b}$ 可得 $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{d}$, 其中 $\mathfrak{c} \sim \mathfrak{o}$ 且 $\mathfrak{d}$ 是整的. 特别, $\mathfrak{a} \sim \mathfrak{b}\mathfrak{d}$.

(13) 由 $\mathfrak{a} \sim \mathfrak{b}$ 可得 $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{d}$, 其中 $\mathfrak{c} \sim \mathfrak{o}$ 且 $\mathfrak{d} \sim \mathfrak{o}$.

这样, 在两个情形下, 有 $\mathfrak{a}(\mathfrak{b}\mathfrak{b}^{-1}) = \mathfrak{b}(\mathfrak{a}\mathfrak{b}^{-1})$.

最大公因子 $(\mathfrak{a}, \mathfrak{b})$ 自然既是 $\mathfrak{a}$ 又是 $\mathfrak{b}$ 的拟因子. 我们现在指出：

(14) $\mathfrak{a}$ 与 $\mathfrak{b}$ 的每一个拟公因子都是 $(\mathfrak{a}, \mathfrak{b})$ 的拟因子. 因为如果 $\mathfrak{c}$ 是这样的一个拟公因子, 那么 $\mathfrak{c}^*$ 是 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的一个公因子, 从而是 $(\mathfrak{a}, \mathfrak{b})$ 的一个因子.

两个整理想 $\mathfrak{a}, \mathfrak{b}$ 叫做*拟无公因子的*, 如果 $(\mathfrak{a}, \mathfrak{b}) \sim \mathfrak{o}$, 或者换句话说, 如果 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的每一个整拟公因子都与 $\mathfrak{o}$ 拟相等.

(15) 如果 $\mathfrak{a}$ 与 $\mathfrak{b}$ 且与 $\mathfrak{c}$ 拟无公因子, 那么也与积 $\mathfrak{b}\mathfrak{c}$ 拟无公因子. 有

$$(\mathfrak{a}, \mathfrak{b}) \cdot (\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}^2, \mathfrak{a}\mathfrak{c}, \mathfrak{b}\mathfrak{a}, \mathfrak{b}\mathfrak{c}) \subseteq (\mathfrak{a}, \mathfrak{b}\mathfrak{c}).$$

左端 $\sim \mathfrak{o}$, 因此右端也必须如此.

我们现在证明属于 Artin 的.

定理 2(加细定理)　*如果一个整理想 $\mathfrak{a}$ 的两个因子分解被给定：*

$$\mathfrak{a} \sim \mathfrak{b}_1\mathfrak{b}_2\cdots\mathfrak{b}_m \sim \mathfrak{c}_1\mathfrak{c}_2\cdots\mathfrak{c}_n, \tag{17.10}$$

那么这两个乘积还可以继续分解, 使得除因子次序及拟相等性外是一致的：

$$\mathfrak{b}_\lambda \sim \prod_\mu \mathfrak{b}_{\lambda\mu},\ \ \mathfrak{c}_\mu \sim \prod_\lambda \mathfrak{b}_{\lambda\mu}. \tag{17.11}$$

证　令 $(\mathfrak{b}_1, \mathfrak{c}_1) = \mathfrak{b}_{11}$. 根据性质 (12). $\mathfrak{b}_1 \sim \mathfrak{b}_{11}\mathfrak{b}_1'$, $\mathfrak{c}_1 \sim \mathfrak{b}_{11}\mathfrak{c}_1'$. 由此得 $\mathfrak{b}_{11} = (\mathfrak{b}_1, \mathfrak{c}_1) \sim (\mathfrak{b}_{11}\mathfrak{b}_1', \mathfrak{b}_{11}\mathfrak{c}_1') = \mathfrak{b}_{11}(\mathfrak{b}_1', \mathfrak{c}_1')$, 从而 $(\mathfrak{b}_1', \mathfrak{c}_1') \sim \mathfrak{o}$. 再令 $(\mathfrak{b}_1', \mathfrak{c}_2) = \mathfrak{b}_{12}$. 根据 (12). $\mathfrak{b}_1' \sim \mathfrak{b}_{12}\mathfrak{b}_1'', \mathfrak{c}_2 \sim \mathfrak{b}_{12}\mathfrak{c}_2'$. 又得到 $(\mathfrak{b}_1'', \mathfrak{c}_2') \sim \mathfrak{o}$. 如此继续进行, 最后得 $\mathfrak{b}_1 = \mathfrak{b}_{11}\mathfrak{b}_{12}\cdots\mathfrak{b}_{1n}\mathfrak{d}$ 及 $\mathfrak{c}_\mu = \mathfrak{b}_{1\mu}\mathfrak{c}_\mu'(\mu = 1, 2, \cdots, n)$. 代入 (17.10), 于是有

$$\mathfrak{b}_{11}\mathfrak{b}_{12}\cdots\mathfrak{b}_{1n}\mathfrak{d}\mathfrak{b}_2\cdots\mathfrak{b}_m \sim \mathfrak{b}_{11}\mathfrak{c}_1'\mathfrak{b}_{12}\mathfrak{c}_2'\cdots\mathfrak{b}_{1n}\mathfrak{c}_n'.$$

根据群的性质 (定理 1), 可以将 $\mathfrak{b}_{11}\cdots\mathfrak{b}_{1n}$ 消去：

$$\mathfrak{d}\mathfrak{b}_2\cdots\mathfrak{b}_m \sim \mathfrak{c}_1'\mathfrak{c}_2'\cdots\mathfrak{c}_n'.$$

这里, $\mathfrak{d}$ 与一切 $\mathfrak{c}_\mu'$, 因而也与乘积 $\mathfrak{c}_1'\mathfrak{c}_2'\cdots\mathfrak{c}_n'$ 拟无公因子. 然而, $\mathfrak{d}$ 作为因子在左端出现, 因此, 它是乘积 $\mathfrak{c}_1'\mathfrak{c}_2'\cdots\mathfrak{c}_n'$ 的一个拟因子. 所以必须 $\mathfrak{d} \sim \mathfrak{o}$, 因而也可以将因子 $\mathfrak{d}$ 略去：

$$\mathfrak{b}_2\cdots\mathfrak{b}_m \sim \mathfrak{c}_1'\mathfrak{c}_2'\cdots\mathfrak{c}_n'.$$

现在可以对 $\mathfrak{b}_2, \cdots, \mathfrak{b}_m$ 进行同样的过程, 直到所说的分解 (17.11) 出现为止.

从现在起一切德文字母都表示异于零理想的整理想. 这样的一个理想 $\mathfrak{p}$ 叫做*不可分解的*, 如果它不与 $\mathfrak{o}$ 拟相等, 并且在每一个乘积表示 $\mathfrak{p} \sim \mathfrak{a}\mathfrak{b}$ 里, 必定有一个

因子属于单位类, 或者根据 (12), 这就是说, 如果 $\mathfrak{p}$ 不与 $\mathfrak{o}$ 拟相等, 并且除去与 $\mathfrak{p}$ 或 $\mathfrak{o}$ 拟相等的拟因子外, 没有其他拟因子.

如果将一个不可分解理想 $\mathfrak{p}$ 代以与它拟相等的最大理想 $\mathfrak{p}^*$, 那么 $\mathfrak{p}^*$ 的每一个整真因子一定不与 $\mathfrak{p}$ 拟相等, 从而与 $\mathfrak{o}$ 拟相等. 根据 (4), 每一个可以被 $\mathfrak{p}$ 或 $\mathfrak{p}^*$ 拟整除的理想都可以被 $\mathfrak{p}^*$ 整除. 于是有

(16) $\mathfrak{p}^*$ 是一个素理想. 这就是说, 如果两个主理想 $\mathfrak{b}$ 与 $\mathfrak{c}$ 的乘积 $\mathfrak{bc}$ 可以被 $\mathfrak{p}^*$ 整除, 但 $\mathfrak{b}$ 不能被 $\mathfrak{p}^*$ 整除, 那么 $(\mathfrak{b},\mathfrak{p}^*)$ 是 $\mathfrak{p}^*$ 的一个真因子, 从而与 $\mathfrak{o}$ 拟相等, 因此

$$\mathfrak{c}=\mathfrak{oc}\sim(\mathfrak{b},\mathfrak{p}^*)\mathfrak{c}=(\mathfrak{bc},\mathfrak{p}^*\mathfrak{c})\geqslant(\mathfrak{p}^*,\mathfrak{p}^*)=\mathfrak{p}^*,$$

所以 $\mathfrak{c}$ 能被 $\mathfrak{p}^*$ 拟整除, 因而被 $\mathfrak{p}^*$ 整除.

如果我们在 $\mathfrak{o}$ 中再假定因子链条件成立, 那么有

(17) 每一个整理想链 $\mathfrak{a}_1>\mathfrak{a}_2>\cdots$, 此处每一个后面的理想都是前一个的真拟因子 (即是拟因子而不拟相等), 在有限多步终止. 因为如果将理想 $\mathfrak{a}_1,\mathfrak{a}_2,\cdots$ 代以与它们拟相等的最大理想 $\mathfrak{a}_1^*,\mathfrak{a}_2^*,\cdots$, 那么就得到一个整理想链 $\mathfrak{a}_1^*\subset\mathfrak{a}_2^*\subset\cdots$, 根据因子链条件, 这个链必定中断.

我们也可以将“拟因子链条件”(17) 表述为“因子归纳原理”(参考 15.1 节, 因子链条件的第四种表述). 根据这个原理, 不难推出, 每一个整理想都与一个不可分解的理想积拟相等. 分解的唯一性是作为加细定理 (定理 2) 的特殊情形得到的. 于是有

定理 3 每一个异于零理想的整理想除因子次序及拟相等性外与唯一确定的不可分解的理想$\mathfrak{p}_1,\mathfrak{p}_2,\cdots,\mathfrak{p}_r$(自然也可以选取素理想 $\mathfrak{p}_1^*,\mathfrak{p}_2^*,\cdots,\mathfrak{p}_r^*$)的积拟相等.

推论 一个理想 $\mathfrak{a}\sim\mathfrak{p}_1\cdots\mathfrak{p}_r$ 可以被 $\mathfrak{b}\sim\mathfrak{p}_1'\cdots\mathfrak{p}_s'$ 拟整除, 当且仅当在 $\mathfrak{b}$ 的分解中出现的每一个因子 $\mathfrak{p}_i'$ 在 $\mathfrak{a}$ 的分解中至少也出现同样多次. 特别, 如果 $\mathfrak{b}$ 是一个主理想, 那么根据 (2), 由拟整除性得出整除性. 如果对 $\mathfrak{a}$ 及 $\mathfrak{b}$ 取主理想 (a) 及 (b), 那么就得到关于 a 被 b 整除或 ab^{-1} 的整性的一个判定标准. 通过非主理想类的引入, 于是就得到由主理想类及非主理想类所组成的一个新领域, 在其中根据定理 (3), 唯一素因子分解成立, 从而达到“古典理想论”的目的.

定理 3 对于分式理想 $\mathfrak{a}b^{-1}$ 也成立. 我们只需将负幂

$$\mathfrak{p}^{-k}=(\mathfrak{p}^{-1})^k$$

也当作因子. 这就是说, 如果

$$\mathfrak{a}\sim\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r}\quad 及\quad (b)=\mathfrak{p}_1^{b_1}\cdots\mathfrak{p}_r^{b_r},$$

于是得

$$\mathfrak{a}b^{-1}\sim\mathfrak{p}_1^{a_1-b_1}\cdots\mathfrak{p}_r^{a_r-b_r}, \tag{17.12}$$

并且指数 a_i-b_i 是唯一确定的.

为了建立现在所得到的理论与一般理想论和 17.4 节中的特殊理想论的关系, 我们需要研究怎样的素理想是不可分解的以及怎样的理想与 $\mathfrak{o}$ 拟相等.

我们已经看到, 对不可分解的 $\mathfrak{p}$ 来说, $\mathfrak{p}^*$ 是素的. 我们现在指出:

(18) 这样的 $\mathfrak{p}^*$ 的任意一个异于零理想的真倍都不是素的. 这就是说, 如果 $\mathfrak{a}$ 是这样的一个真倍, 那么 $\mathfrak{a}\geqslant\mathfrak{p}^*$. 根据 (12), 有 $\mathfrak{a}\mathfrak{c}=\mathfrak{p}^*\mathfrak{d}$, 其中 $\mathfrak{c}\sim\mathfrak{o}$. 因为在 $\mathfrak{d}$ 的分解中比 $\mathfrak{a}$ 的分解中少出现一个素因子, 所以 $\mathfrak{d}\not\equiv 0(\mathfrak{a})$. 同样 $\mathfrak{p}^*\not\equiv 0(\mathfrak{a})$, 然而 $\mathfrak{p}^*\mathfrak{d}\equiv 0(\mathfrak{a})$. 所以 $\mathfrak{a}$ 不是素理想.

现在考察一个任意素理想 $\mathfrak{p}$ 的分解. 或者 $\mathfrak{p}\sim\mathfrak{o}$, 或者在分解 $\mathfrak{p}\sim\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r$ 中有一个不可分解因子 $\mathfrak{p}_1$ 出现. 这时 $\mathfrak{p}\geqslant\mathfrak{p}_1$, 所以 $\mathfrak{p}\subseteq\mathfrak{p}_1^*$. 然而 $\mathfrak{p}_1^*$ 的一个真倍不能是素的, 所以必须 $\mathfrak{p}=\mathfrak{p}_1^*$. 于是 $\mathfrak{p}^*=(\mathfrak{p}_1^*)=\mathfrak{p}_1^*=\mathfrak{p}$. 由此得

(19) 每一个素理想 $\mathfrak{p}$ 或者与 $\mathfrak{o}$ 拟相等或者不可分解并且等于相应的 $\mathfrak{p}^*$.

在第二个情形, $\mathfrak{p}$ 没有异于零理想的真素倍. 反过来, 我们证明, 在前一情形, 这样的一个倍确实存在.

(20) 如果 $\mathfrak{p}\sim\mathfrak{o}$, 那么存在 $\mathfrak{p}$ 的一个不可分解的真素倍 $\mathfrak{p}_\nu^*$. 事实上, 如果 $p\neq 0$ 是 $\mathfrak{p}$ 的一个元素且 $(p)\sim\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r\sim\mathfrak{p}_1^*\mathfrak{p}_2^*\cdots\mathfrak{p}_r^*$ 是它的分解, 那么由 (2) 得 $\mathfrak{p}_1^*\mathfrak{p}_2^*\cdots\mathfrak{p}_r^*\equiv 0(p)\equiv 0(\mathfrak{p})$, 从而有一个 $\mathfrak{p}_\nu^*\equiv 0(\mathfrak{p})$. 然而 $\mathfrak{p}_\nu^*\neq\mathfrak{p}$, 因为否则将有 $\mathfrak{p}_\nu^*\sim\mathfrak{o}$.

我们说一个素理想是*较高位的*, 如果它没有异于零理想的真素倍; 反过来, 如果它有一个这样的素倍理想, 那么就说是*低位的*. 于是可以将 (18)~(20) 合并为

定理 4 *每一个高位素理想 $\mathfrak{p}$ 是不可分解的并且等于它的 $\mathfrak{p}^*$; 每一个低位素理想都与 $\mathfrak{o}$ 拟相等.*

根据分解定理 (定理 3), 一个理想, 如果不属于单位类, 那么它至少能被一个高位素理想 $\mathfrak{p}=\mathfrak{p}^*$ 整除. 然而单位类的一个理想不能被任何高位素理想整除. 因此, 这就提供了单位类的一个纯理想论 (即在整理想范围内) 的刻画.

根据公理 II, 在 17.4 节所考虑的环内, 一个异于 (0) 的素理想只被它本身及 $\mathfrak{o}$ 整除. 因此, 在这个环里除 $\mathfrak{o}$ 外不存在任何低位素理想. 因为每一理想 $\mathfrak{a}\neq\mathfrak{o}$ 可以被一个异于 $\mathfrak{o}$ 的素理想整除 (证: 在 $\mathfrak{a}$ 的异于 $\mathfrak{o}$ 的因子中找出一个最大的, 它是无因子的, 因而是素的), 所以 $\mathfrak{a}$ 不能与 $\mathfrak{o}$ 拟相等. 因此单位类仅由单位理想 $\mathfrak{o}$ 组成. 于是由 (12) 进一步得出, 拟整除性与整除性的意义是一样的, 由此或由 (13), 同样拟相等与相等的意义也是一样的. 于是 17.4 节的理想论作为特例被包括在现在所叙述的理论中.

对于一般理想论的关联也容易建立. 首先容易看出, 每一个准素理想, 如果属于它的素理想是一个低位理想, 那么它一定与 $\mathfrak{o}$ 拟相等. 我们将这种准素理想特别记作*低位准素理想*, 而其余的准素理想记作*高位准素理想*. 一个理想与 $\mathfrak{o}$ 拟相等, 必要且只要它的一切准素分支都是低位的. 如果两个理想 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的所有高位的 (不

一定低位的) 准素分支一致, 那么它们拟相等. 在与 $\mathfrak{a}$ 拟相等的理想中找出一个最大理想 $\mathfrak{a}^*$. 它可以从分解 $\mathfrak{a}=[\mathfrak{q}_1,\cdots,\mathfrak{q}_r]$ 中去掉一切低位的准素分支而得到. 因此, 本节的分解定理与唯一性定理可以如此解释, 即始终略去一切低位准素分支而只注意高位准素分支. 高位准素理想只能被一个高位素理想整除, 从而根据定理 2, 在它的因子分解里必定产生一个素理想幂, 这就是说, *每一个高位准素理想与一个素理想幂拟相等*.

反过来, 每一个高位素理想的幂也与一个高位准素理想拟相等. 事实上, 如果 $\mathfrak{a}=\mathfrak{p}^r$ 是一个高位素理想的幂, 那么 $\mathfrak{a}$ 不能被 $\mathfrak{p}$ 以外的高位素理想所整除, 因而在分解

$$\mathfrak{a}=\mathfrak{p}^r=[\mathfrak{q}_1,\cdots,\mathfrak{q}_r]$$

中只有一个高位准素理想出现. 例如, 设这个高位准素理想是 $\mathfrak{q}_1$, 那么 $\mathfrak{a}^*=\mathfrak{q}_1$. 从而 $\mathfrak{a}=\mathfrak{p}^r$ 与准素理想 $\mathfrak{q}_1$ 拟相等.

此外, $\mathfrak{q}_1$ 恰是在 15.6 节所定义的素理想 $\mathfrak{p}$ 的 r 次符号幂. 因此, *高位准素理想恰是高位素理想的符号幂*.

按照 Prüfer 的说法, 具有性质 $\mathfrak{a}^*=\mathfrak{a}$ 的理想 $\mathfrak{a}$ 叫做 v 理想. 整 v 理想恰是这样的理想, 在它们的准素理想分解中只有高位准素理想出现. 一切主理想都是 v 理想. 在每一个拟相等理想类中存在一个唯一的 v 理想 $\mathfrak{a}_\nu=\mathfrak{a}^*$. 如果我们按照 Prüfer 及 Krull 那样只限于 v 理想, 那么拟相等的概念是多余的. 这时主要定理 (定理 3) 可以如此叙述:

每一个 v 理想可以唯一地表示成高位素理想的符号幂 $\mathfrak{p}^{(r)}$ 的交.

习题 17.11 这一节的一切结果对于有零因子的环也成立, 只要我们将商域代以商环并且限于考虑非零因子理想.

习题 17.12 由定理 1 反过来可得环 $\mathfrak{o}$ 的整闭性 (参考 17.5 节).

习题 17.13 证明 $\mathfrak{a}:\mathfrak{b}\sim\mathfrak{a}\mathfrak{b}^{-1}$[①].

理想论概要

以下的总结指出在 16.3 节中所叙述的公理 I(因子链条件), II(每一素理想是无因子的), III(整闭性) 对于整环的理想论的意义:

由 I, 每一理想都是准素理想的最小公倍, 所属的素理想是唯一的.

由 I 与 II, 每一理想都是单素准素理想的积, 并且是唯一的.

由 I 与 III, 每一理想都与一个素理想幂积拟相等, 除拟相等性外是唯一的.

由 I~III, 每一理想都是素理想幂的积; 唯一的.

① 关于这一节的结果的进一步一般化可以看 Prüfer H. *J. reine und angew. Math., Bd.*, 1932, 168 及 Lorenzen P. *Math. Z., Bd.*, 1939, 45.

第 18 章　赋　值　域

18.1　赋　　值

11.2 节中所给出的由一个给定的有序域 K 作出域 Ω 的作法, 并没有完全利用到域 K 中的顺序, 而仅利用到域元素 a 的绝对值 $|a|$ 的顺序. 这就使我们想到作更进一步的研究, 将这一作法拓广到有序域以外的其他域去, 只要这种域中存在着具有绝对值的性质的一个函数 $\varphi(a)$.

一个域 K 称为赋值域, 如果对 K 中的元素 a 定义了一个函数 $\varphi(a)$, 它具有下面的性质：

(1) $\varphi(a)$ 是某一有序域中的元素;

(2) 对 $a \neq 0$ 有 $\varphi(a) > 0$; $\varphi(0) = 0$;

(3) $\varphi(ab) = \varphi(a)\varphi(b)$;

(4) $\varphi(a+b) \leqslant \varphi(a) + \varphi(b)$.

由 (2) 和 (3) 立即可以推出

$$\varphi(1) = 1, \quad \varphi(-1) = 1, \quad \varphi(a) = \varphi(-a).$$

在 (4) 中命 $c = a + b$ 可得

$$\varphi(c) - \varphi(a) \leqslant \varphi(c - a).$$

另一方面, 由同样方式可得

$$\varphi(a) - \varphi(c) \leqslant \varphi(c - a).$$

因此有

$$|\varphi(c) - \varphi(a)| \leqslant \varphi(c - a).$$

当 b 被换成 $-b$ 时, 不等式 (4) 也成立, 这样就得到

$$\varphi(a - b) \leqslant \varphi(a) + \varphi(b).$$

利用完全归纳法很容易将 (4) 中的不等式推广到 n 个项的和. 每个域有一个 “平凡” 赋值 $\varphi(a) = 1$(对$a \neq 0$) 以及 $\varphi(0) = 0$. 我们以后排除这种赋值.

如果 K 本身是一个有序域, 可命 $\varphi(a)=|a|$. 不过存在完全不同的赋值. 设 $\mathbb{Q}$ 是有理数域. 设 p 是某一固定的素数, 并将每个有理数 $a\neq 0$ 写成

$$a=\frac{s}{t}p^n$$

的形式, 其中 s 和 t 是不能被 p 整除的整数, 那么令

$$\varphi_p(a)=p^{-n},\quad \varphi_p(0)=0,$$

就可定义 $\mathbb{Q}$ 的一个赋值. (1)~(3) 非常容易验证.

代替 (4), 我们有更强的不等式

$$\varphi_p(a+b)\leqslant \max(\varphi_p(a),\varphi_p(b)). \tag{18.1}$$

事实上, 设

$$a=\frac{s}{t}p^n,\quad b=\frac{u}{v}p^m,\quad s,t,u,v \text{ 与 } p \text{ 互素},$$

并设 $\varphi_p(b)\geqslant\varphi_p(a)$, 即 $n\geqslant m$, 则有

$$a+b=\frac{svp^{n-m}+tu}{tv}p^m,$$

因而

$$\varphi_p(a+b)=p^{-m'},\quad \text{其中} m'\geqslant m,$$

即

$$\varphi_p(a+b)\leqslant\varphi_p(b).$$

这就是 $\mathbb{Q}$ 的 p-adic 赋值.

p-adic 赋值的概念不难加以推广. 设 $\mathfrak{o}$ 是一个整环, K 是它的商域, $\mathfrak{p}$ 是 $\mathfrak{o}$ 中一个具有下列性质的素理想:

(A) 各个幂 $\mathfrak{p},\mathfrak{p}^2,\cdots$ 互不相同, 且其交为零理想.

(B) 设 $\mathfrak{o}$ 中的 a 恰被 $\mathfrak{p}^\alpha$ 整除, 即能被 $\mathfrak{p}^\alpha$ 整除但不能被 $\mathfrak{p}^{\alpha+1}$ 整除, 而 b 恰被 $\mathfrak{p}^\beta$ 整除, 则 ab 恰被 $\mathfrak{p}^{\alpha+\beta}$ 整除.

这里 $\mathfrak{p}^\alpha$ 表示所有和 $\sum\limits_{\nu}p_{\nu 1}p_{\nu 2}\cdots p_{\nu\alpha}$ 的全体, 而所有的 $p_{\nu\kappa}$ 都是 $\mathfrak{p}$ 中元素. 特别 $\mathfrak{p}^1=\mathfrak{p},\mathfrak{p}^0=\mathfrak{o}$. 现在我们给出如下的定义: 设 $\mathfrak{o}$ 中的元素 a 恰被 $\mathfrak{p}^\alpha$ 整除, 则命

$$\varphi(a)=e^{-\alpha},\quad \text{而 } \varphi(0)=0,$$

其中 e 是任意一个 >1 的实数. 这样, 赋值 $\varphi(a)$ 就对 $\mathfrak{o}$ 中的元素有了定义, 并且具有性质 (1)~(4).

另一方面, 当一个赋值对整环中的元素有了定义时, 由

$$\varphi\left(\frac{a}{b}\right)=\frac{\varphi(a)}{\varphi(b)}$$

立即可以将它开拓到商域中的元素上去. 这样一个定义是单值的, 因为由

$$\frac{a}{b}=\frac{c}{d}\quad \text{或}\ ad=bc$$

即有

$$\varphi(a)\varphi(d)=\varphi(b)\varphi(c)\quad \text{或}\ \frac{\varphi(a)}{\varphi(b)}=\frac{\varphi(c)}{\varphi(d)}.$$

其次, 赋值 $\varphi\left(\frac{a}{b}\right)$ 也具有性质 (1)~(4). 前三个性质是自明的. 性质 (4) 可证明如下：

$$\begin{aligned}\varphi\left(\frac{a}{b}+\frac{c}{d}\right)=\frac{\varphi(ad+bc)}{\varphi(bd)}&\leqslant\frac{\varphi(ad)+\varphi(bc)}{\varphi(bd)}\\&=\varphi\left(\frac{a}{b}\right)+\varphi\left(\frac{c}{d}\right).\end{aligned}$$

这样, 我们就从整环 $\mathfrak{o}$ 中由素理想 $\mathfrak{p}$ 所确定的赋值出发得出了商域 K 的一个赋值. 这个赋值称为 K 的 $\mathfrak{p}$-adic 赋值.

特别, 当 $\mathfrak{p}$ 是整环 $\mathfrak{o}$ 的非零真素理想, 并且满足 17.4 节的 3 条公理时, 性质 (A) 与 (B) 都满足. 每一个这样的素理想 $\mathfrak{p}$ 都可以定义商域 K 的一个 $\mathfrak{p}$-adic 赋值. 特别可应用于代数数域的代数整数环里的素理想. 这显示了经典理想论与赋值论的密切联系.

更进一步, 根据 17.7 节, 我们可以从仅满足公理 I 和 III 的整环 $\mathfrak{o}$ 出发, 只考虑 17.7 节意义下的高位素理想 $\mathfrak{p}$, 并且构作 15.6 节意义下的符号幂

$$\mathfrak{q}=\mathfrak{p}^{(r)},$$

它具有以下类似于 (A) 和 (B) 的性质：

(A′) $\mathfrak{p}^{(r)}$ 互不相同, 它们的交是零理想;

(B′) 若 $\mathfrak{a}$ 恰好被 $\mathfrak{p}^{(r)}$ 整除, $\mathfrak{b}$ 恰好被 $\mathfrak{p}^{(s)}$ 整除, 则 $\mathfrak{ab}$ 恰好被 $\mathfrak{p}^{(r+s)}$ 整除.

如果 $\mathfrak{a}$ 恰好被 $\mathfrak{p}^{(r)}$ 整除, 我们又可以定义

$$\varphi(\mathfrak{a})=e^{-r}\quad \text{以及}\ \varphi(0)=0.$$

这样就对每个高位素理想 $\mathfrak{p}$ 得到了一个 $\mathfrak{p}$-adic 赋值.

在多项式环 $\Delta[x_1,\cdots,x_n]$ 中, 理想

$$\mathfrak{p}=(x_1,\cdots,x_n)$$

也具有性质 (A) 和 (B). 这样得出来的赋值 $\varphi(f)$ 即 $e^{-\alpha}$, 其中 α 是出现在 f 中的最低次项的次数.

习题 18.1　在赋值的定义中去掉 $\varphi(a)$ 不取负值的要求, 证明：如果在 K 中有一个元素 c, 使得 $\varphi(c) < 0$, 则 $a \to \varphi(a)$ 是把 K 映成值域 P 的一个子域的一个同构映射 (将不等式 (4) 应用于 $\varphi(ac + bc)$, 从而证明 (4) 中的等号成立).

习题 18.2　在 $\mathfrak{p}$-adic 赋值的情形下, 条件 (4) 可改进为 (18.1).

赋值域的一些最重要的研究, 都是和值域 P 为阿基米德有序域的情形有关的. 在这一情形下, 根据习题 11.6, P 可以嵌到实数域中去. 因此, 我们从现在起假定值 $\varphi(a)$ 都是实数. 在这里我们假定读者知道实数的 (自然) 对数, 对数的一些最简单的性质以及一个正数 α 以任意实数为指数的幂 α^{β}.

此外, 我们还要用到下面这样一个关于实数的引理：

引理　*如果 α, β, γ 是任意正实数, 且对任意自然数 ν 有*

$$\gamma^{\nu} \leqslant a\nu + \beta,$$

则 $\gamma \leqslant 1$.

证　设 $\gamma = 1 + \delta, \delta > 0$, 那么当 $\nu \geqslant 2$ 时将有

$$\begin{aligned}\gamma^{\nu} = (1+\delta)^{\nu} &= 1 + \nu\delta + \frac{1}{2}\nu(\nu-1)\delta^2 + \cdots \\ &> \nu\delta + \frac{1}{2}\nu(\nu-1)\delta^2.\end{aligned}$$

但当 ν 足够大时, 必有

$$\nu\delta > \beta \quad 和 \quad \frac{1}{2}(\nu-1)\delta^2 > \alpha,$$

故得

$$\gamma^{\nu} > \beta + \alpha\nu,$$

而这是与所设相违的.

域 K 的一个实数赋值 $\varphi(a)$ 称为非阿基米德的, 如果对单位元素的任意整数倍 $n = 1 + 1 + 1 + \cdots + 1$, 有

$$\varphi(n) \leqslant 1.$$

有理数域 $\mathbb{Q}$ 的 p-adic 赋值就是一个非阿基米德赋值, 在这里值域为阿基米德域这一事实不起任何作用.

域 K 的赋值 φ 为非阿基米德赋值, 当且仅当代替 4. 有更强的不等式

(4′) $\varphi(a+b) \leqslant \max(\varphi(a), \varphi(b))$

成立.

证　(1) 如果 (4′) 对两个被加项的情形成立, 那么相应的不等式对 n 个项的和也成立. 特别, 对于 $n = 1 + 1 + \cdots + 1$, 有

$$\varphi(n) \leqslant \max(\cdots, \varphi(1), \cdots) = 1.$$

(2) 如果 φ 是非阿基米德赋值, 则当 $\nu = 1, 2, 3, \cdots$ 时,

$$\begin{aligned}(\varphi(a+b))^\nu = \varphi((a+b)^\nu) &= \varphi\left(a^\nu + \binom{\nu}{1}a^{\nu-1}b + \cdots + b^\nu\right)\\ &\leqslant \varphi(a)^\nu + \varphi(a)^{\nu-1}\varphi(b) + \cdots + \varphi(b)^\nu\\ &\leqslant (\nu+1)M^\nu,\end{aligned}$$

其中 $M = \max(\varphi(a), \varphi(b))$. 根据前面的引理可知

$$\frac{\varphi(a+b)}{M} \leqslant 1, \quad \text{即 } \varphi(a+b) \leqslant M.$$

这就证明了 $(4')$.

在今后, 即使值域 P 不是由实数组成的, 我们也把不等式 $(4')$ 看作是一个非阿基米德赋值的标志. 正如 Krull 所指出的那样, 在这一场合下, 可以取任意有序 Abel 群作为取值范围, 因为我们只需要将不同的值相乘, 以及比较值的大小, 不同值相加的运算根本不会遇到.

下面的一点注记经常是很有用的, 这个注记适用于所有在上面定义的意义下的非阿基米德赋值.

如果 $\varphi(a)$ 和 $\varphi(b)$ 不相等, 则 $(4')$ 中等号成立.

证　不妨设 $\varphi(a) > \varphi(b)$. 我们要证明

$$\varphi(a+b) = \varphi(a).$$

假如

$$\varphi(a+b) < \varphi(a),$$

那么 $\varphi(a+b)$ 和 $\varphi(-b) = \varphi(b)$ 都小于 $\varphi(a)$. 但这是和不等式

$$\varphi(a) \leqslant \max(\varphi(a+b), \varphi(-b))$$

相矛盾的.

对于非阿基米德赋值, 引进另外一种记法经常是比较方便的 (在文献中也常是这样作的). 我们不直接考虑实数值 $\varphi(a)$, 而考虑指数 $w(a) = -\log\varphi(a)$. 考虑指数时, 赋值的定义关系将成为：

(1) 当 $a \neq 0$ 时, $w(a)$ 是一个实数;

(2) $w(0)$ 是记号 ∞;

(3) $w(ab) = w(a) + w(b)$;

(4) $w(a+b) \geqslant \min(w(a), w(b))$.

在这种场合下我们就说所考虑的赋值是一个**指数赋值**. 我们之所以能够过渡到考虑指数, 是由于较强的不等式 (4′) 使得我们没有必要将值 $\varphi(a)$ 相加. 对数变换倒转了值的顺序并将乘法改变为加法.

例　设域 K 中的元素是 z 平面上的, 或者更一般些, 是某一 Riemann 面上一个区域中的单值解析 (亚纯) 函数. 我们取 Riemann 面上一个固定的点 P, 并作如下的定义：函数 a 的赋值 $w(a)$ 等于 α, 如果它以 P 点为一个 α 阶零点; 等于零, 如果它在 P 点取不等于零的有限值; 等于 $-\alpha$, 如果它以 P 点为 α 阶极点. 这时性质 (1)~(4) 都能成立. 这样一来, 相应于每个点 P 都有域 K 的一个赋值. 这个例子说明赋值论在一个复变量的代数函数论中的意义.

我们将指数赋值分为两种类型. **离散赋值**：这种赋值的特征是存在一个最小的正值 $w(a)$, 而所有其他可能出现的值 $w(a)$ 都是它的整数倍 (参看上面的例子); **非离散赋值**：在这种赋值中可能出现的值 $w(a)$ 能够和值零接近到任意程度. 由于一个值 $w(a)$ 的整数倍仍是一个值 $nw(a) = w(a^n)$, 故在非离散赋值的情形下值 $w(a)$ 在实数集合中处处稠密.

有理数域的 p-adic 赋值是离散的, 所有的 $\mathfrak{p}$-adic 赋值也同样是离散的.

在一个指数赋值的域 K 中, 满足条件 $w(a) \geqslant 0$ 的元素组成一个环 $\mathfrak{I}$. 事实上, 由 $w(a) \geqslant 0$ 和 $w(b) \geqslant 0$ 可得 $w(a \pm b) \geqslant \min(w(a), w(b)) \geqslant 0$ 和 $w(ab) = w(a) + w(b) \geqslant 0$. K 中满足条件 $w(a) > 0$ 的元素的全体 $\mathfrak{p}$ 是 $\mathfrak{I}$ 中的一个素理想. 事实上, 首先由 $w(a) > 0$, $w(b) > 0$ 可得 $w(a \pm b) \geqslant \min(w(a), w(b)) > 0$, 因而 $\mathfrak{p}$ 是一个模. 其次, 由 $a \in \mathfrak{p}$, 即 $w(a) > 0$ 和 $w(c) \geqslant 0$ 可得 $w(ca) = w(c) + w(a) > 0$, 故 $\mathfrak{p}$ 是一个理想. 最后, 由 $ab = 0(\mathrm{mod}\ \mathfrak{p})$, 即由 $w(ab) = w(a) + w(b) > 0$ 可知 $w(a)$ 和 $w(b)$ 二数中至少必有一个为正, 也就是说, a 和 b 两个元素中必有一个可被 $\mathfrak{p}$ 整除, $\mathfrak{p}$ 是一个素理想.

$\mathfrak{I}$ 称为赋值 w 的**赋值环**. $\mathfrak{I}$ 中的元素称为整元素 (相对于赋值 w 来说的). 如果 a/b 是整元素, 即 $w(a) \geqslant w(b)$, 我们就说元素 a 能被元素 b 整除 (相对于赋值 w 来说).

满足条件 $w(a) = 0$ 的元素就是环 $\mathfrak{I}$ 中的可逆元素. 由于 $\mathfrak{I}$ 中不属于 $\mathfrak{p}$ 的元素都是可逆元素, 故 $\mathfrak{p}$ 是 $\mathfrak{I}$ 中的一个极大理想. 这样一来, 同余类环 $\mathfrak{I}/p$ 就是一个域, 称为赋值 w 的**剩余类域**. 如果域 K 的特征是 p, 则剩余类域的特征也是 p. 如果域 K 的特征为零, 则剩余类域的特征可以是零 (特征相等的情形), 也可以是某一素数 (特征不相等的情形). 特征不相等情形的一个典型的例子就是 p-adic 赋值. 如果我们将一个不定元添加到有理数域上去, 并将一个有理函数的指数赋值定义为分母的次数和分子的次数之差, 那么就得到特征相等情形的一个例子. 多项式环 $K[x_1, \cdots, x_n]$ 中通过一个素理想定义的 $\mathfrak{p}$-adic 赋值 (参看上文) 也属于特征相

等的情形.

关于这些概念的进一步讨论, 直到所有赋值的完全分类, 可参看 Hasse, Schmidt, Teichmüller 和 Witt①的工作. 关于赋值概念的推广可参看 Mahler 和 Krull 的工作②.

习题 18.3 证明: $\mathfrak{I}$ 中的每个理想或者是所有满足条件 $w(a) > \delta$ 的元素 a 的集合, 或者是所有满足条件 $w(a) \geqslant \delta$ 的元素的集合, 其中 δ 为一非负实数. 对于离散赋值可以仅限于 $\geqslant$ 的情形, 而其中的 δ 则是一个的确在值的集合中出现的数. 在非离散赋值的情形 δ 由理想所唯一确定.

习题 18.4 在离散赋值的情形 $\mathfrak{I}$ 中所有的理想都是 $\mathfrak{p}$ 的幂. 与此相反, 在非离散赋值的情形 $\mathfrak{p}$ 的各次幂都和 $\mathfrak{p}$ 相等.

18.2 完 备 扩 张

对于每个赋值域 K, 我们可以利用 11.2 节中所述的程序作出一个扩域 Ω_K, 使得在它里面 Cauchy收敛定理成立. 为此假设 $\varphi(a)$ 的取值是实数. 现在我们通过下面的性质定义 K 中的一个基本序列 $\{a_\nu\}$:

$$\varphi(a_p - a_q) < \varepsilon, \quad \text{当} \quad p > n(\varepsilon), \quad q > n(\varepsilon),$$

其中 ε 是任意正实数. 由基本序列环可以作出同余类域 Ω_K, 其作法和 11.2 节中的作法完全相同, 所有的证明也可以逐字逐句借用. 唯一的差别就是现在的域 K 和域 Ω_K 不再是有序的, 而仅是赋值的, Ω_K 的赋值定义如下: 如果 α 由基本序列 $\{a_\nu\}$ 决定, 那么根据前面已经证明的不等式

$$|\varphi(a_\nu) - \varphi(a_\mu)| \leqslant \varphi(a_\nu - a_\mu),$$

值 $\varphi(a_\nu)$ 也构成一个基本列, 因而在实数域中有一个极限. 我们命

$$\varphi(\alpha) = \omega$$

具有同一极限 α 的基本序列决定同一值 $\varphi(\alpha)$, 这个值满足要求 (1) $\sim$ (4).

相对于赋值 φ 来说域 Ω_K 是完备的, 也就是说, Cauchy 收敛准则成立:

定理 *Ω_K 中的每个基本序列在 Ω_K 中有极限.*

我们已经说过一个序列 $\{a_\nu\}$ 是一基本序列, 如果对值域中的任意 $\varepsilon > 0$ 可以找到一个 n, 使得当 $p > n, q > n$ 时

① Witt E I. *reine u. angew. Math.*, 1936, 176: 126–140 以及所引文献.

② Mahler K. Über Pseudobewertunge, I.. *Acta Math.*, 1936, 66: 79–199; Ia. *Akad Wetensch. Amsterdam, Proc.*, 1936, 39: 57–65; II. *Acta Math.*, 1936, 67: 51–80. –Krull W. Allgemeine bewertungstheorie. J. *Reine Angew. Math.*, 1932, 167: 160–196.

$$\varphi(a_p - a_q) < \varepsilon.$$

在非阿基米德赋值的情形, 代替这样一个条件只需要求当 $\nu > n(\varepsilon)$ 时,

$$\varphi(a_{\nu+1} - a_\nu) < \varepsilon$$

就够了.

事实上, $a_p - a_q$ 是 $|p-q|$ 个项 $a_{\nu+1} - a_\nu$ 的和, 如果所有这些项的值都 $< \varepsilon$, 则根据 (18.1), 它们的和的值也 $< \varepsilon$.

因此, *在一个完备的非阿基米德赋值域中, 只要差 $a_{\nu+1} - a_\nu$ 构成一个零序列, 序列 $\{a_\nu\}$ 就有极限.*

这个准则也可以叙述如下: *无穷级数 $a_1 + a_2 + a_3 + \cdots$ 收敛的充分必要条件是 $\lim a_\nu = 0$.*

如果我们用普通的绝对值来给有理数域 $\mathbb{Q}$ 赋值: $\varphi(a) = |a|$, 那么所得到的完备扩张自然就是实数域. 如果我们从 $\mathbb{Q}$ 的 p-adic 赋值出发, 则所得到的完备扩张就是 Hensel 的 p-adic 数域 Ω_p.

这样, 域 $\Omega_2, \Omega_3, \Omega_5, \Omega_7, \Omega_{11}, \cdots$ 就是一批在实数域之外的同等的完备域 (对于算术理论来说, 也是同样重要的).

域 Ω_p 中的元素, 即 p-adic 数, 除了可以表成基本序列之外, 还有一种更加方便的表示方法. 对 $\lambda = 0, 1, 2, 3, \cdots$ 我们考虑分子能被 p^λ 整除而分母不能被 p 整除的有理数, 即满足条件 $\varphi(a) \leqslant p^{-\lambda}$ 的有理数所组成的模 $\mathfrak{M}_\lambda$. 如果两个有理数之差属于 $\mathfrak{M}_\lambda$, 我们就说这两个数同余 (mod p^λ). 现在设 $\{r_\mu\}$ 是一个由有理数组成的 p-adic 基本序列, 那么对于每个 λ 从某一足数 $n = n(\lambda)$ 起将会有

$$\varphi(r_\mu - r_\nu) \leqslant p^{-\lambda}, \quad \text{当} \quad \mu > n(\lambda), \quad \nu > n(\lambda),$$

即有

$$r_\mu \equiv r_\nu (\text{mod } p^\lambda).$$

因此, 当 $\mu > n(\lambda)$ 时, 所有的数 r_μ 都属于模 $\mathfrak{M}_\lambda$ 的同一个同余类 $\mathfrak{R}_\lambda$. 这样, 基本序列 $\{r_\mu\}$ 决定一个同余类的序列:

$$\mathfrak{R}_0 \supset \mathfrak{R}_1 \supset \mathfrak{R}_2 \subset \mathfrak{R}_3 \supset \mathfrak{R}_4 \supset \cdots,$$

这些同余类象这里所写出的那样, 是一个包含在另一个之内的. 反之, 如果一个序列 $\{r_1, r_2, \cdots\}$ 决定出模 $\mathfrak{M}_\lambda$ 的同余类 $\mathfrak{R}_\lambda$ 的一个包含在另一个之内的一个同余类序列 $\{\mathfrak{R}_\lambda\}$, 使得

$$r_\mu \in \mathfrak{R}_\lambda \quad \text{对所有} \quad \mu > n(\lambda),$$

那么它就是一个基本序列.

特别, 如果 $\{r_\mu\}$ 是零基本序列, 那么 $\mathfrak{R}_\lambda = \mathfrak{M}_\lambda$ 就是零同余类. 两个基本序列相加时: $\{r_\mu\}+\{s_\mu\}=\{r_\mu+s_\mu\}$, 相应的同余类序列也相加: $\{\mathfrak{R}_\lambda+\mathfrak{S}_\lambda\}$. 特别, 当我们把一个零基本序列加到另一个基本序列上去时, 相应的同余类序列不改变. 反之, 如果两个基本序列属于同一个同余类序列 $\{\mathfrak{R}_\lambda\}$, 则它们的差是零基本序列. 因此, 每给一个 p-adic 数 $\alpha = \lim r_\nu$ 有一个上述类型的同余类序列和它一一地相对应.

将 p-adic 数表成同余类序列, 这就是上面所提到的比较方便的表示方法. 为了从 p-adic 数 α 的同余类序列表示得出它的一个 (特殊的) 基本序列, 只要从每个同余类 $\mathfrak{R}_\lambda$ 中取出一个数 r'_λ 就行. 这时必有 $\alpha = \lim r'_\lambda$. α 也可以表成一个无限和: 命

$$r'_1 = s_0, \quad r'_{\lambda+1} - r'_\lambda = s_\lambda p^\lambda,$$

则

$$r'_{\lambda+1} = s_0 + s_1 p + s_2 p^2 + \cdots + s_\lambda p^\lambda,$$

因此

$$\alpha = \lim_{\lambda\to\infty} \sum_{\nu=0}^{\lambda} s_\nu p^\nu = \sum_{\nu=0}^{\infty} s_\nu p^\nu, \tag{18.2}$$

这里的 $s_1, s_2, \cdots$ 是分母不能被 p 整除的有理数.

普通整数的 p-adic 极限称为 p-adic整数. 对同余类 $\mathfrak{R}_0, \mathfrak{R}_1, \cdots$ 来说, 这就意味着每个这样的同余类当中都可以找到一个整数. 特别, 在 p-adic 整数的情形, $\mathfrak{R}_0$ 就是零同余类 $\mathfrak{M}_0$, 即分母不能被 p 整除的有理数的全体. 另一方面, 这一条件也是使得一个 p-adic 数为 p-adic 整数的充分条件: 如果 $\mathfrak{R}_0$ 是模 $\mathfrak{M}_0$ 的零同余类, 则所有同余类 $\mathfrak{R}_1, \mathfrak{R}_2, \cdots$ 包含有整数. 事实上, $\mathfrak{R}_\lambda$ 包含在 $\mathfrak{R}_0$ 之内, 因而完全由形为 $\dfrac{r}{s}, s \not\equiv 0 (\bmod\ p)$ 的数组成. 解同余式

$$sx = r \pmod{p^\lambda},$$

则有

$$x - \frac{r}{s} = \frac{sx-r}{s} \equiv 0 \pmod{\mathfrak{M}_\lambda}.$$

因此整数 x 属于同余类 $\mathfrak{R}_\lambda$.

由于这个原因, 当 α 为 p-adic 整数时, 在级数表示 (18.2) 中可取所有的 r'_λ, 因而可取所有的 s_λ 为普通整数. 这样一来, (18.2) 就是 p 的一个带整系数的幂级数. 每个这样的幂级数都在 p-adic 赋值的意义下收敛, 因而表示一个 p-adic 整数.

具有同余类序列表示 $\{\mathfrak{R}_0, \mathfrak{R}_1, \cdots\}$ 的每个 p-adic 数 α 都可以乘上 p 的一个幂成为一个 p-adic 整数. 事实上, 设 r'_0 是同余类 $\mathfrak{R}_0$ 中的一个元素, 那么将 r'_0 和

p 的一个幂 p^m 相乘之后, 可使得 $p^m r_0'$ 的分母不再含有因子 p, 即 $p^m r_0'$ 属于模 m_0 的零同余类. 现在, 如果将 p-adic 整数 $p^m\alpha$ 展成带有整系数 $s_0, s_1, \cdots$ 的幂级数 (18.2), 就可得到 α 的一个幂级数表示, 其中出现有限多个带负指数的项：

$$\alpha = a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots . \tag{18.3}$$

p-adic 整数 α 的表示式 (18.2) 可加以规范化, 即每将都取 r_λ' 为同余类 $\mathfrak{R}_\lambda$ 中最小的非负整数. 这时所有整数 s_ν 都满足条件 $0 \leqslant s_\nu < p$. 现在再由 (18.2) 过渡到 (18.3), 我们就得到*每个 p-adic 数的一个唯一地确定的展开式* (18.3), 其中 $0 \leqslant a_\nu < p$.

在 18.1 节中我们曾经描述过怎样由一个整环 $\mathfrak{o}$ 中的素理想 $\mathfrak{p}$ 定义一个域 K 中的一个 $\mathfrak{p}$-adic 赋值. 由这个 $\mathfrak{p}$-adic 赋值可以得出一个完备的 *$\mathfrak{p}$-adic 域* $\Omega_{\mathfrak{p}}$, 这就是 Hensel p-adic 域的一个推广. 举例来说, 如果 $\mathfrak{p}$ 是多项式整环 $\Delta[x]$ 中的理想 $(x-c)$, 则 $\Omega_{\mathfrak{p}}$ 就是所有幂级数

$$\alpha = a_{-m}(x-c)^{-m} + \cdots + a_0 + a_1(x-c) + a_2(x-c)^2 + \cdots \tag{18.4}$$

的域, 幂级数的系数 a_ν 属于 Δ. 不论系数 a_ν 如何选择, 这个幂级数在 $\mathfrak{p}$-adic 赋值的意义之下永远是收敛的. 我们把算式 (18.4) 称为 *$x-c$ 的形式幂级数*.

习题 18.5　将 -1 和 $1/2$ 表成规范化的 3-aidc 幂级数.

习题 18.6　设 f 为一整系数多项式. 方程 $f(\xi)=0$ 在域 Ω_p 中可解, 当且仅当对每个自然数 n 同余式

$$f(\xi) = 0 (\mathrm{mod}\ p^n)$$

有一个有理解 ξ.

习题 18.7　方程

$$x^2 = -1, \quad x^2 = 3, \quad x^2 = 7$$

在域 Ω_3 中是否可解?

可能出现这样的情况, 即域 K 的两个不同的赋值 φ 和 ψ 决定同一个完备扩域 Ω. 显然可见, 这样一种情况出现, 当且仅当 K 中的每一序列 $\{a_\nu\}$ 对 φ 来说为一零基本序列时, 对 ψ 来说也是零基本序列, 反之亦然. 在这样一种情况下, 即当 $\lim\limits_{\nu\to\infty} \varphi(a_\nu) = 0$ 和 $\lim\limits_{\nu\to\infty} \psi(a_\nu) = 0$ 的意义完全相同时, 我们说赋值 φ 和 ψ 等价.

对于复数域的普通绝对值赋值 $\varphi(a) = |a|$, 只要命 $\varphi(a) = |a|^\rho$, 其中 ρ 是不大于 1 的任意正实数, 就可作出无限多个和它等价的赋值. 条件 (1) $\sim$ (3) 显然成立. 条件 (4) 可由 $|a+b| \leqslant |a| + |b|$ 和不等式 $\varepsilon^\rho + \delta^\rho \geqslant (\varepsilon+\delta)^\rho$ 推出, 这个不等式对任意两个实数 $\varepsilon \geqslant 0, \delta \geqslant 0$ 和任意 $0 < \rho \leqslant 1$ 成立①.

对有理数域的 p-adic 赋值 $\varphi_p(a)$ 来说, 每个赋值 $\psi(a) = \varphi_p(a)^\sigma$ 都和它等价, 其中 σ 表示任意一个固定的正数.

① 参看 Hardy-Littlewood-Polya. *Inequalities* (不等式). Cambridge, 1934, 第 2 章.

设 φ 和 ψ 是域 K 的两个赋值. 我们将证明以下三个断言等价：

(1) φ 和 ψ 等价;

(2) $\varphi(a)<1$ 蕴含 $\psi(a)<1$;

(3) ψ 是 φ 的幂, 即 $\psi(a)=\varphi(a)^{\varepsilon}$ 对所有的 a 以及取定的 $\varepsilon>0$ 成立.

首先证明断言 (1) 蕴含 (2). 这里 $\varphi(a)<1$ 蕴含 a^n 在赋值 φ 的意义下收敛于零. 于是 a^n 也必须在赋值 ψ 的意义下收敛于零. 因此 $\psi(a)<1$.

再证明断言 (2) 蕴含 (3). 注意到 $\varphi(a)<\varphi(b)$ 蕴含 $\varphi\left(\dfrac{a}{b}\right)<1$. 这就意味着 $\psi(a/b)<1$ 或 $\psi(a)<\psi(b)$. 现在设 p 是 K 中任意一个固定的元素, 它使得 $\varphi(p)>1$. 这时也必有 $\psi(p)>1$. 设 a 是 K 中任意一个元素, 且 $\varphi(a)=\varphi(p)^{\delta}$, $\psi(a)=\psi(p)^{\delta'}$. 我们要证明 $\delta=\delta'$. 设 n 和 m 是满足条件 $n/m\leqslant\delta$ 与 $m>0$ 的两个整数, 那么有

$$\varphi(p)^{n/m}<\varphi(p)^{\delta}=\varphi(a),\quad \text{因而}\quad \varphi(p^n)<\varphi(a^m),$$

从这里即得

$$\psi(p^n)<\psi(a^m),\quad \psi(p)^{n/m}<\psi(a)=\psi(p)^{\delta'},\quad n/m<\delta'.$$

由于所有满足条件 $n/m<\delta$ 的分数 n/m 的上确界即 δ, 故有 $\delta\leqslant\delta'$. 同样可知 $\delta'\leqslant\delta$, 因而 $\delta=\delta'$. 注意 $\varepsilon=\dfrac{\log\psi(p)}{\log\varphi(p)}$ 是一个和 a 无关的正数, 并且由于对所有的 a 都有 $\delta=\delta'$, 故有

$$\log\psi(a)=\delta'\log\psi(p)=\delta\log\psi(p)=\delta\varepsilon\log\varphi(p)=\varepsilon\log\varphi(a),$$

因此

$$\psi(a)=\varphi(a)^{\varepsilon}.$$

断言 (3) 蕴含 (1) 是显然的. 因此 (1), (2) 和 (3) 是等价的.

设域 K 带有赋值 φ, 赋 K' 和 K 同构且带有赋值 ψ. 我们说 K 和 K' 之间的同构是*双方连续的或拓扑的*, 如果 K 中的每个 φ 零序列被这个同构映成 K' 中的一个 ψ 零序列, 并且反之亦然. 在这一情形下, 域 K 和 K' 称为*连续同构的*. 在一个拓扑同构之下, 收敛序列和收敛序列、基本序列和基本序列相互对应. 由此立即可以得出下面的结论：

定理 *连续同构的赋值域 K 和 K' 具有连续同构的完备扩域 Ω_K 和 $\Omega_{K'}$.*

习题 18.8 证明：我们所知道的有理数域的各种赋值, 即绝对值赋值和 p-adic 赋值之中, 没有两个赋值是等价的.

18.3 有理数域的赋值

下面这个由 Ostrowski 所首先证明的定理说明, 我们所知道的有理数域的赋值, 即绝对值赋值和 p-adic 赋值, 本质上就是全部可能的赋值. 在这里我们仍旧假定值域就是实数域.

定理 有理数域 $\mathbb{Q}$ 的一个非平凡的赋值或者是 $\varphi(a) = |a|^\rho$, 其中 $0 < \rho \leqslant 1$, 因而和绝对值赋值等价; 或者是 $\varphi(a) = \varphi_p(a)^\sigma$, 其中 p 为固定素数, σ 为一固定正数, 因而和一个 p-adic 赋值等价.

证 对每个有理整数 n, 有

$$\varphi(n) \leqslant |n|.$$

事实上, 有

$$\begin{aligned}\varphi(n) &= \varphi(1 + 1 + \cdots + 1) \\ &\leqslant \varphi(1) + \varphi(1) + \cdots + \varphi(1) = |n|.\end{aligned}$$

现设 $a > 1, b > 1$ 是两个有理整数. 我们将 b^ν 按 a 的幂展开

$$\begin{gathered}b^\nu = c_0 + c_1 a + \cdots + c_n a^n, \\ 0 \leqslant c_\nu < a, \quad c_n \neq 0.\end{gathered}$$

所出现的 a 的最高次幂 a^n 最多等于 b^ν:

$$a^n \leqslant b^\nu,$$

即

$$n \leqslant \nu \frac{\log b}{\log a}.$$

命 $M = \max(1, \varphi(a))$. 由于

$$\begin{aligned}\varphi(b^\nu) &\leqslant \varphi(c_0) + \varphi(c_1)\varphi(a) + \cdots + \varphi(c_n)\varphi(a)^n \\ &< a(1 + \varphi(a) + \cdots + \varphi(a)^n) \leqslant a(n+1)M^n,\end{aligned}$$

故有

$$\varphi(b)^\nu < a\left(\frac{\log b}{\log a}\nu + 1\right) M^{(\log b/\log a)\nu},$$

或

$$\left(\frac{\varphi(b)}{M^{(\log b/\log a)}}\right)^\nu < a\frac{\log b}{\log a}\nu + a.$$

根据 18.1 节的引理, 从这里可得

$$\varphi(b) \leqslant M^{\frac{\log b}{\log a}},$$

即

$$\varphi(b) \leqslant \max\left(1, \varphi(a)^{\frac{\log b}{\log a}}\right).$$

第一种情形　φ 为阿基米德赋值. 这时必有一整数 b, 使得 $\varphi(b) > 1$. 如果对于任意另外某个整数 $a > 1$ 有 $\varphi(a) \leqslant 1$, 则由刚才所证不等式将会得出矛盾 $\varphi(b) \leqslant 1$. 因此, 对所有整数 $a > 1$ 有 $\varphi(a) > 1$. 在这一情形上述不等式可写成

$$\varphi(b) \leqslant \varphi(a)^{\frac{\log b}{\log a}}$$

或

$$\varphi(b)^{\frac{1}{\log b}} \leqslant \varphi(a)^{\frac{1}{\log a}}.$$

另一方面, a 和 b 的地位是可以交换的, 因此也有

$$\varphi(a)^{\frac{1}{\log a}} \leqslant \varphi(b)^{\frac{1}{\log b}},$$

从而得

$$\varphi(a)^{\frac{1}{\log a}} = \varphi(b)^{\frac{1}{\log b}}.$$

如果 $\varphi(b) = b^{\rho}$, 那么由这个等式就可知 $\varphi(a) = a^{\rho}$, 因而对每个有理数 $r = \dfrac{a}{b}$,

$$\varphi(r) = |r|^{\rho}.$$

由于 $\varphi(a) < 1$, 故 $\rho > 0$; 又由于

$$2^{\rho} = \varphi(2) = \varphi(1+1) \leqslant \varphi(1) + \varphi(1) = 2,$$

故必有 $\rho \leqslant 1$.

第二种情形　φ 为非阿基米德赋值, 因而对所有整数 a, $\varphi(a) \leqslant 1$. 满足条件 $\varphi(a) < 1$ 的整数 a 的全体显然是整数环中的一个理想. 这个理想是素的, 因为由 $\varphi(ab) = \varphi(a)\varphi(b) < 1$ 必有 $\varphi(a) < 1$ 或 $\varphi(b) < 1$. 我们知道, 整数环中每个理想都是主理想, 特别每个素理想都由一个素数生成. 因此, 满足条件 $\varphi(a) < 1$ 的整数 a 恰恰就是某一素数 p 的所有倍数. 每个有理数 r 都可以表成 $r = \dfrac{z}{n}p^{\rho}$ 的形式, 其中 n 和 z 都不能被 p 整除. 由于 $\varphi(z) = \varphi(n) = 1$, 故有 $\varphi(r) = \varphi(p)^{\rho} = p^{-\rho\sigma} = \varphi_p(r)^{\sigma}$, 这里 $\sigma = -\dfrac{\log \varphi(p)}{\log p}$ 是一个固定的数, 并且由于 $\varphi(p) < 1$, 这个数是正的. 所以赋值 φ 等价于 p-adic 赋值 φ_p.

有理数域 $\mathbb{Q}$ 的赋值完全确定之后, 我们可以进一步考虑代数扩域和超越扩域. 先从代数扩域入手.

这里我们主要限于考虑非阿基米德赋值：阿基米德赋值的意义比较小. 事实上, Ostrowski 曾经证明, *任何一个阿基米德赋值域 K 都和一个由复数组成而以普通绝对值赋值的域连续同构*. 关于这个定理的证明可以参看 Ostrowski 的原作[①].

因此, 我们为自己提出如下的一个纲领：假设已经给定了域 K 的一个 (非阿基米德) 赋值 φ. 我们考虑 K 的一个代数扩域 Λ, 并提出这样的问题：域 K 的赋值 φ 能不能且有多少种方式可以开拓成域 Λ 的赋值 Φ.

在 18.4 节中我们假定 K 是一个完备的赋值域. 在 18.5 节中, 我们通过嵌入的办法将非完备赋值域的情形归结为完备的情形. 在 18.6 节中我们利用所得到的结果来确定一个任意的代数数域的所有阿基米德与非阿基米德赋值.

习题 18.9 设 $\varphi_0(a) = |a|$ 而 $\varphi_p(a)$ 是 p-adic 赋值, 则对每个固定的元素 a 所有这些值的积等于 1.

18.4 代数扩域的赋值：完备情形

设域 K 对指数赋值 $w(a) = -\log\varphi(a)$ 来说是完备的, 即在 K 中 Cauchy 收敛准则成立. 我们要研究怎样把这个指数赋值开拓到 K 的代数扩域 Λ 上去.

让我们再提醒一次, 满足条件 $w(a) \geqslant 0$ 的元素 a 称为*整元素*, 它们组成一个环; 满足条件 $w(a) > 0$ 的元素 a 组成这个环中的一个素理想 $\mathfrak{p}$.

由 Hensel 所建立的、完备域中的一个*可约性准则*, 乃是下面的研究的基础.

设指数赋值域中多项式

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

的系数当中 a_ν 的指数最小, 那么多项式

$$\frac{a_n}{a_\nu}x^n + \frac{a_{n-1}}{a_\nu}x^{n-1} + \cdots + \frac{a_0}{a_\nu}$$

的系数全是整的, 并且不全属于 $\mathfrak{p}$. 这样一个多项式称为一个*本原多项式*.

Hensel 引理 *设 K 对指数赋值 w 是完备的. $f(x)$ 是以 K 中整元素为系数的一个本原多项式. 如果 $g_0(x)$ 和 $h_0(x)$ 是以 K 中整元素为系数的多项式, 并且条件*

$$f(x) \equiv g_0(x)h_0(x) \pmod{\mathfrak{p}}$$

① Ostrowski A. Über einige Lösungen der Funktionalgleichung $\varphi(x)\varphi(y) = \varphi(x, y)$(论函数方程 $\varphi(x)\varphi(y) = \varphi(xy)$ 的某些解). *Acta Math.*, 1918, 41: 271–284. Ostrowski 发表在*Math. Z.*, 1934, 39: 296–404 的另一长篇论文乃是下文的基础.

成立, 那么可以找到两个以 K 中整元素为系数的多项式 $g(x)$ 和 $h(x)$, 使得

$$\begin{aligned} &f(x)=g(x)h(x), \\ &g(x)\equiv g_0(x) \pmod{\mathfrak{p}}, \\ &h(x)\equiv h_0(x) \pmod{\mathfrak{p}}, \end{aligned}$$

这里假定 $g_0(x)$ 和 $h_0(x)$ 是模 $\mathfrak{p}$ 互素的. 除此之外, $g(x)$ 和 $h(x)$ 还可以这样选择, 使得 $g(x)$ 的次数等于 $g_0(x)$ 模 $\mathfrak{p}$ 的次数.

证 由于我们可以从 $g_0(x)$ 和 $h_0(x)$ 中去掉能被 $\mathfrak{p}$ 整除的系数, 而不影响整个引理的条件与结论, 故可事先假定 $g_0(x)$ 是一个 r 次多项式, 且 $g_0(x)$ 和 $h_0(x)$ 的首项系数都是可逆元素. 此外, 当我们把 $g_0(x)$ 换成 $\dfrac{1}{a}g_0(x), h_0(x)$ 换成 $ah_0(x)$ 时, 也不会产生任何影响. 因此可以假定 $g_0(x)$ 是一个规范化的 r 次多项式, 即其首项系数等于 $1: g(x)=x^r+\cdots$. 这样一来, 如果 $h_0(x)$ 的首项系数为 b, 次数为 s, 则乘积 $g_0(x)h_0(x)$ 的首项系数等于 b, 而其次数等于 $r+s\leqslant n$. 现在我们要作出多项式 $g(x)$ 和 $h(x)$, 使得 $g(x)$ 是一个 r 次的规范化多项式, 从而 $h(x)$ 是一个 $n-r$ 次多项式.

根据我们的假设, 多项式 $f(x)-g_0(x)h_0(x)$ 的系数全都具有正的指数. 设其中最小者为 $\delta_1>0$. 如果 $\delta_1=\infty$, 则 $f(x)=g_0(x)h_0(x)$, 那就没什么要证明的了.

由于 $g_0(x)$ 和 $h_0(x)$ 模 $\mathfrak{p}$ 互素, 故可找到两个以 K 中整元素为系数的多项式 $l(x)$ 和 $m(x)$, 使得

$$l(x)g_0(x)+m(x)h_0(x)\equiv 1 \pmod{\mathfrak{p}}.$$

设多项式

$$l(x)g_0(x)+m(x)h_0(x)-1$$

的系数当中最小的指数为 $\delta_2>0$, 并设 δ_1,δ_2 二数中较小者为 ε, 最后设 π 是满足条件 $w(\pi)=\varepsilon$ 的元素, 则有

$$f(x)\equiv g_0(x)h_0(x) \pmod{\pi}, \tag{18.5}$$

$$l(x)g_0(x)+m(x)h_0(x)\equiv 1 \pmod{\pi}. \tag{18.6}$$

我们所要造的多项式 $g(x)$ 是一串 r 次多项式 $g_\nu(x)$ 的极限, 其中第一个多项式是 $g_0(x)$; $h(x)$ 是一串次数 $\leqslant n-r$ 的多项式 $h_\nu(x)$ 的极限, 其中第一个多项式是 $h_0(x)$. 假设 $g_\nu(x)$ 和 $h_\nu(x)$ 已经造出, 且满足条件

$$f(x)\equiv g_\nu(x)h_\nu(x) \pmod{\pi^{\nu+1}}, \tag{18.7}$$

$$g_\nu(x) \equiv g_0(x) \pmod{\pi}, \tag{18.8}$$

$$h_\nu(x) \equiv h_0(x) \pmod{\pi}, \tag{18.9}$$

而 $g_\nu(x) = x^r + \cdots$ 的首项系数为 1. 为了造出 $g_{\nu+1}(x)$ 和 $h_{\nu+1}(x)$, 我们先试命

$$g_{\nu+1}(x) = g_\nu(x) + \pi^{\nu+1}u(x), \tag{18.10}$$

$$h_{\nu+1}(x) = h_\nu(x) + \pi^{\nu+1}v(x). \tag{18.11}$$

这时就有

$$\begin{aligned} g_{\nu+1}(x)h_{\nu+1}(x) - f(x) =& g_\nu(x)h_\nu(x) - f(x) \\ & + \pi^{\nu+1}\{g_\nu(x)v(x) + h_\nu(x)u(x)\} + \pi^{2\nu+2}u(x)v(x). \end{aligned}$$

根据 (18.7), 可命

$$f(x) - g_\nu(x)h_\nu(x) = \pi^{\nu+1}p(x),$$

这样便得

$$\begin{aligned} g_{\nu+1}(x)h_{\nu+1}(x) - f(x) \equiv& \pi^{\nu+1}\{g_\nu(x)v(x) \\ & + h_\nu(x)u(x) - p(x)\} \pmod{\pi^{\nu+2}}. \end{aligned}$$

为了使得左端能被 $\pi^{\nu+2}$ 整除, 只需满足同余式

$$g_\nu(x)v(x) + h_\nu(x)u(x) \equiv p(x) \pmod{\pi} \tag{18.12}$$

即可.

为了达到这一目的, 我们将同余式 (18.6) 乘以 $p(x)$,

$$p(x)l(x)g_0(x) + p(x)m(x)h_0(x) \equiv p(x) \pmod{\pi}, \tag{18.13}$$

以 $g_0(x)$ 除 $p(x)m(x)$, 其剩余 $u(x)$ 为一次数 $< r$ 的多项式：

$$p(x)m(x) = q(x)g_0(x) + u(x), \tag{18.14}$$

将 (18.14) 代入 (18.13) 得

$$\{p(x)l(x) + q(x)h_0(x)\}g_0(x) + u(x)h_0(x) \equiv p(x) \pmod{\pi},$$

将花括号中所有能被 π 整除的系数都换成 0, 就得到

$$v(x)g_0(x) + u(x)h_0(x) \equiv p(x) \pmod{\pi}. \tag{18.15}$$

由于 (18.8) 和 (18.9), 由 (18.15) 即得所要求的同余式 (18.12). 其次, $u(x)$ 的次数 $< r$, 因此, 由 (18.10) 可知 $g_{\nu+1}(x)$ 和 $g_\nu(x)$ 有相同的次数和首项系数. 现在只要证明 $v(x)$ 的次数 $\leqslant n-r$ 就行了. 假如不是这样的话, (18.15) 的第一项中将会出现一个次数 $>n$ 的最高次项, 而其余各项的次数都不大于 n. 因此, 根据 (18.15), 这个最高次项的系数能被 π 整除, 从而 $v(x)$ 的首项系数能被 π 整除. 另一方面, 由于 $v(x)$ 的系数当中能被 π 整除的均已去掉, 故知 $v(x)$ 的次数 $\leqslant n-r$.

在上面我们已经看到, 由同余式 (18.12) 即有

$$f(x) \equiv g_{\nu+1}(x)h_{\nu+1}(x) \pmod{\pi^{\nu+2}}. \tag{18.16}$$

由 (18.10) 可以看出, 多项式 $g_{\nu+1}(x)-g_\nu(x)$ 的系数能被 $\pi^{\nu+1}$ 整除, 因此, 当 $\nu\to\infty$ 时, 这些系数的极限是零. 根据 Cauchy 收敛准则可知, 当 $\nu\to\infty$ 时, $g_\nu(x)$ 收敛于一个多项式

$$g(x) = x^r + \cdots .$$

同样, 当 $\nu\to\infty$ 时, $h_\nu(x)$ 收敛于一个多项式 $h(x)$. 最后, 在 (18.7) 中取极限即得

$$f(x) = g(x)h(x),$$

而由 (18.8) 和 (18.9) 取极限可得

$$g(x) = g_0(x) \pmod{\mathfrak{p}},$$

$$h(x) = h_0(x) \pmod{\mathfrak{p}}.$$

推论　如果

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

是 K 中的不可约多项式, 则

$$\min(w(a_0), w(a_1), \cdots, w(a_n)) = \min(w(a_0), w(a_n)).$$

为了证明这一点, 我们假定 $f(x)$ 是本原的. 这时 $\min(w(a_0),\cdots,w(a_n))$ 等于零. 假如 $w(a_0)$ 和 $w(a_n)$ 都大于零, 那么一定有一个 $r, 0<r<n$, 使得 $w(a_r)=0$, 而当 $v=r+1,\cdots,n$ 时 $w(a_\nu)>0$. 这样一来, 便有

$$f(x) \equiv (a_0 + a_1x + \cdots + a_rx^r)\cdot 1 \pmod{\mathfrak{p}}$$
$$0<r<n.$$

因此, 根据 Hensel 引理, $f(x)$ 可分解一个 r 次因子和一个 $n-r$ 次因子.

习题 18.10 如果一个多项式 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ 以 K 中整元素为系数, 并且模 $\mathfrak{p}$ 不可约, 那么 $f(x)$ 在完备域 Ω_K 中也是不可约的.

习题 18.11 如果在 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ 中所有系数 $a_{n-1}, \cdots, a_0$ 都属于 $\mathfrak{p}$, 并且 a_0 不能表成 $\mathfrak{p}$ 中两个元素的积, 则 $f(x)$ 是不可约的 (Eisenstein 不可约准则的推广).

习题 18.12 试研究有理数域中的不可约多项式

$$x^2+1, \quad x^2+2, \quad x^2-3$$

在 3-adic 数域中的因子分解问题 (利用习题 18.10, Hensel 引理和习题 18.11).

最后, 这个定理的一个最重要的应用就是证明完备指数赋值 w 可以开拓到代数扩域上去.

定理 设域 K 对指数赋值 w 来说是完备的, Λ 是 K 的一个代数扩域, 那么可以作出域 Λ 的一个指数赋值 W, 使得它在 K 上和 w 一致.

证 (1) 设 ξ 是 Λ 中的一个元素, 而

$$\xi^n + a_{n-1}\xi^{n-1} + \cdots + a_0 = 0$$

是 ξ 所满足的系数属于 K 的不可约方程. 我们断言

$$W(\xi) = \frac{1}{n}w(a_0)$$

是 Λ 的一个赋值 (这个赋值在 K 上显然和 w 一致). 为了对 Λ 中的两个元素 ξ 和 η 证明关系式

$$W(\xi\eta) = W(\xi) + W(\eta),$$

$$W(\xi+\eta) \geqslant \min(W(\xi), W(\eta)),$$

我们考虑子域 $\Lambda_0 = K(\xi, \eta)$, 这个子域在 K 上有有限次数 t. 我们在这个子域中作 ξ 的范数. 根据 6.11 节, 有

$$N(\xi) = (-1)^t a_0^r, \quad r = \frac{t}{n},$$

因此

$$w(N(\xi)) = w(a_0^r) = rw(a_0),$$

$$W(\xi) = \frac{1}{n}w(a_0) = \frac{1}{t}w(N(\xi)).$$

由于 $N(\xi\eta) = N(\xi)N(\eta)$, 故从这里立即得出

$$W(\xi\eta) = W(\xi) + W(\eta).$$

证明不等式 $W(\xi+\eta) \geqslant \min(W(\xi), W(\eta))$ 时, 由于

$$W(\xi+\eta) = W(\eta) + W\left(1 + \frac{\xi}{\eta}\right)$$

和

$$\min(W(\xi), W(\eta)) = W(\eta) + \min\left(W\left(\frac{\xi}{\eta}\right), 0\right),$$

我们可以仅限于 $\eta = 1$ 的情形.

另一方面, $\xi+1$ 所满足的不可约方程是

$$(\xi+1)^n + \cdots + (a_0 - a_1 + a_2 - \cdots + (-1)^{n-1}a_{n-1} + (-1)^n) = 0,$$

因而根据前面的定理, 的确有

$$\begin{aligned} W(\xi+1) &= \frac{1}{n} w(a_0 - a_1 + \cdots) \\ &\geqslant \frac{1}{n} \min(w(a_0), w(a_1), \cdots, w(a_{n-1}), w(1)) \\ &= \frac{1}{n} \min(w(a_0), w(1)) = \min(W(\xi), 0). \end{aligned}$$

由指数赋值 $w(a), W(\xi)$ 过渡到普通赋值

$$\varphi(a) = e^{-w(a)}, \quad \varPhi(\xi) = e^{-W(\xi)}$$

时, 扩张 $\varLambda$ 的赋值由公式

$$\varPhi(\xi) = \sqrt[n]{\varphi(a_0)}$$

确定; 当 $\varLambda$ 对 K 的次数为有限数 m 时, 由公式

$$\varPhi(\xi) = \sqrt[m]{\varphi(N_\varLambda(\xi))}$$

确定.

我们指出, 完全同样的公式在阿基米德赋值的情形也成立. 唯一的非平凡的情况就是 K 为实数域而 $\varLambda$ 为复数域的情形. K 的赋值

$$\varphi(\xi) = |\xi|^\rho$$

显然可以开拓成 $\varLambda$ 的赋值

$$\varPhi(\xi) = |\xi|^\rho.$$

但现在, 对 $\xi = a + bi$, 有

$$|\xi| = \sqrt{a^2+b^2} = \sqrt{N(\xi)} = \sqrt{|N(\xi)|},$$

故

$$\Phi(\xi) = |\xi|^{\rho} = \sqrt{\varphi(N(\xi))}.$$

由于这样一个情况, 从现在起我们又把阿基米德赋值和非阿基米德赋值放在一起考虑.

设域 Λ 对域 K 的次数是有限的, 而 $u_1, u_2, \cdots, u_n$ 是 Λ/K 的一个基, 并设 K 对赋值 φ 来说是完备的. 如果 Φ 是 Λ 的一个赋值, 它在 K 上和 φ 相一致, 那么 Λ 中的一个序列

$$c_{\nu} = a_1^{(\nu)} u_1 + \cdots + a_n^{(\nu)} u_n, \quad \nu = 1, 2, 3, \cdots$$

对 Φ 来说是一个基本序列, 当且仅当 n 个序列 $\{a_i^{(\nu)}\}$ 对 φ 来说是基本序列.

由于序列 $a_i^{(\nu)}$ 在 K 中分别收敛于极限 a_i, 故知 Λ 对 Φ 来说是完备的.

证　序列 $\{a_i^{(\nu)}\}$ 的收敛性可以用完全归纳法证明如下：如果序列 c_{ν} 具有形式

$$c_{\nu} = a_1^{(\nu)} u_1,$$

那么只要 $\{c_{\nu}\}$ 是一个基本序列, 序列 $\{a_1^{(\nu)}\}$ 也自然是一个基本序列. 现在假设上述断言对所有形为

$$c_{\nu} = \sum_{i=1}^{m-1} a_u^{(\nu)} u_i$$

的序列已经证明, 并设已经给定了一基本序列

$$c_{\nu} = \sum_{i=1}^{m} a_i^{(\nu)} u_i.$$

如果序列 $\{a_m^{(\nu)}\}$ 收敛, 则 $\{c_{\nu} - a_m^{(\nu)} u_m\}$ 也是基本序列, 因而根据归纳假设, 序列 $\{a_i^{(\nu)}\}, i < m$ 收敛, 现在假设 $\{a_m^{(\nu)}\}$ 不收敛, 那么我们可以选择一个自然数序列 $n_1, n_2, n_3, \cdots$, 使得对所有的 v, 有 $\varphi(a_m^{(\nu)} - a_m^{(\nu+n_{\nu})}) > \varepsilon$, 其中 ε 为一固定正数. 序列

$$d_{\nu} = \frac{c_{\nu} - c_{\nu+n_{\nu}}}{a_m^{(\nu)} - a_m^{(\nu+n_{\nu})}} = \sum_{i=1}^{m-1} \frac{a_i^{(\nu)} - a_i^{(\nu+n_{\nu})}}{a_m^{(\nu)} - a_m^{(\nu+n_{\nu})}} u_i + u_m = \sum_{i=1}^{m-1} b_i^{(\nu)} u_i + u_m$$

必趋向零. 事实上, 由于 $\{c_{\nu}\}$ 是一个基本序列, 分子的序列必趋向零. 有

$$d_{\nu} - u_m = \sum_{i=1}^{m-1} b_i^{(\nu)} u_i.$$

根据归纳假设, 序列 $\{b_i^{(\nu)}\}$ 收敛于极限 b_i, 并有

$$-u_m = \sum_{i=1}^{m-1} b_i u_i,$$

然而这是与 $u_1, \cdots, u_n$ 为 Λ/K 的基这一事实相违背的.

用完全同样的办法可以证明, 序列 $\{c_\nu\}$ 为零序列, 当且仅当序列 $\{a_i^{(\nu)}\}(i = 1, \cdots, n)$ 为零序列.

在这样一点注意的基础之上可以证明下面的唯一性定理:

定理　*完备域 K 的赋值 φ 到代数扩张 Λ 上的开拓 Φ 是唯一地确定的, 且有*

$$\Phi(\xi) = \sqrt[n]{\varphi(N(\xi))},$$

其中的范数 $N(\xi)$ 是在域 $K(\xi)$ 中作出的, 而 n 是 $K(\xi)$ 对 K 的次数.

证　只要考虑一个固定的元素 ξ 及与之相应的域 $K(\xi)$ 就行了, 所考虑的范数都是指的在这个域中作出的范数. 如果这个域中一个序列 $\{c_\nu\}$ 趋向零 (在 Φ 的意义下), 那么, 根据上面所述, 当我们将 c_ν 通过 $K(\xi)$ 的基元素 $u_1, \cdots, u_n$ 线性地表出时, 表示式中的系数 $a_i^{(\nu)}$ 也将趋向零. c_ν 的范数是这些系数的齐次多项式, 因此这些范数也趋向零. 现在假设 $\Phi(\xi)^n < \varphi(N(\xi))$ 或 $\Phi(\xi)^n > \varphi(N(\xi))$. 我们分别考虑

$$\eta = \frac{\xi^n}{N(\xi)} \quad 或 \quad \eta = \frac{N(\xi)}{\xi^n}.$$

在两种情形下都有 $N(\eta) = 1$ 和 $\Phi(\eta) < 1$. 因此 $\lim \eta^\nu = 0$, 从而 $\lim N(\eta^\nu) = 0$. 然而这是和 $N(\eta^\nu) = N(\eta)^\nu = 1$ 这一事实相违背的.

习题 18.13　完备赋值域 K 的两个赋值代数扩域 Λ 和 Λ' 之间的一个同构, 如果它使得 K 的元素不动的话, 必将 Λ 的赋值变为 Λ' 的赋值.

习题 18.14　复数域只有一个赋值 Φ, 它在实数域上和 $\varphi(a) = |a|^\rho$ 相一致. 这个赋值就是 $\Phi(a) = |a|^\rho$.

18.5　代数扩域的赋值：一般情形

设 K 是一个任意的赋值域, Λ 是 K 的一个代数扩域. 我们问：能不能和有多少种方式可以将 K 中给定的赋值 φ 开拓成 Λ 的一个赋值.

为了表述简单起见, 我们先只限于考虑单纯扩域 $\Lambda = K(\vartheta)$ 的情形, 并设 ϑ 是 $K[t]$ 中的不可约多项式 $F(t)$ 的零点.

我们先将域 K 扩张成完备赋值域 Ω, 然后再作多项式 $F(t)$ 在 Ω 之上的分裂域 Σ. 根据 18.4 节, Ω 的赋值 φ 可唯一开拓到 Σ 上去.

所谓域 Λ 到域 Σ 之内的一个嵌入, 指的就是一个同构 σ, 它将 $\Lambda = K(\vartheta)$ 映成 Σ 的一个子域 $\Lambda' = K(\vartheta')$, 而使得基域 K 的元素不动. 同构 σ 将 ϑ 映成 $F(t)$ 的一个零点 ϑ', 并且 σ 完全由 ϑ' 确定. 我们断言:

Λ 到 Σ 之内的每个嵌入决定 Λ 的一个赋值. 事实上, Λ' 作为 Σ 的一个子域来看自然是赋值的, 而同构 σ^{-1} 将 Λ' 的赋值转移为 Λ 的赋值. 显然, 这样得到的 Λ 的赋值乃是 K 的赋值 φ 的一个开拓.

我们断言：

Λ 的每一个赋值, 如果它是 K 的赋值 φ 的开拓的话, 都可通过上述方式由 Λ 到 Σ 之内的嵌入得出.

证　我们作出 Λ 的完备扩张. 这个完备扩张包含着 K 的完备扩张 Ω, 并且包含着 ϑ, 因而包含着域 $\Omega(\theta)$. 另一方面, $\Omega(\vartheta)$ 可以扩张成多项式 F 的一个和 Σ 同构的分裂域. 这一同构将 $\Omega(\vartheta)$ 映成 Σ 的一个子域 $\Omega(\theta')$, 而使得 Ω 中的元素不动, 因而将 $\Omega(\theta)$ 的赋值转移成 $\Omega(\theta')$ 中的唯一可能的赋值.

对上面的证明来说, 单纯扩域的限制是完全无关紧要的. 如果不是考虑一个代数量 θ, 而是有限多个代数量 $\zeta_1, \zeta_2, \cdots, \zeta_r$, 且这些代数量分别是 $K[x]$ 中的多项式 $g_1, \cdots, g_r$ 的零点, 那么我们可取乘积 $g_1 \cdots g_r$ 的分裂域作为 Σ, 然后和上面一样地进行推论. 如果 Λ 是 K 的一个无限代数扩域, 则可取 Ω 的代数封闭扩域作为 Σ. 证明仍旧和上面一样.

现在让我们仍旧返回来考虑单纯扩张的情形, 并在 $\Omega[t]$ 中将定义多项式 $F(t)$ 分解成不可约因子

$$F(t) = F_1(t)F_2(t)\cdots F_s(t). \tag{18.17}$$

$K(\vartheta)$ 的每个同构 σ 将 ϑ 映成某一多项式 $F_\nu(t)$ 的一个零点. 相应于每个 $F_\nu(t)$ 都有一个扩域 $\Omega(\vartheta_\nu)$, 其中 ϑ_ν 是 $F_\nu(t)$ 的任意一个零点：究竟是哪一个零点是没有差别的, 因为一个不可约多项式的所有零点都是相互共轭的.

如果一个同构 σ 将元素 ϑ 映成 ϑ_ν, 而使得 K 中的元素不动, 那么它就将每个多项式 $g(\vartheta)$ 映成 $g(\vartheta_\nu)$, 故 σ 由 ϑ_ν 所完全决定. 因此, $\Lambda = K(\vartheta)$ 到 Σ 之内的一切可能的嵌入由对应

$$\vartheta \to \vartheta_\nu \quad (\nu = 1, \cdots, s)$$

决定. 这样一来, Λ 的赋值也就随之决定：要想得到任意某个元素 $\eta = g(\vartheta)$ 的值, 先作出它的第 ν 个共轭元素

$$\eta_\nu = g(\vartheta_\nu),$$

然后根据 18.4 节计算这个共轭元素的值

$$\Phi(\eta_\nu) = \sqrt[n_\nu]{\varphi(N(\eta_\nu))}, \tag{18.18}$$

其中 n_ν 是多项式 F_ν 的次数, 而范数 $N(\eta_\nu)$ 则是在域 $\Omega(\theta_\nu)$ 中作出的. 因此

赋值 φ 的开拓的个数恰等于多项式 $F(t)$ 在 $\Omega[t]$ 中的不可约因子的个数.

18.6 代数数域的赋值

前一节中的一般理论在代数数域的例子上得到了非常出色的说明.

设 $\Lambda = \mathbb{Q}(\vartheta)$ 是一个代数数域, 即将一个本原元素 ϑ 添加于有理数域 $\mathbb{Q}$ 而得到的一个有限扩域, 并设 $F(x)$ 是以 ϑ 为零点的规范化的不可约多项式.

如果将等价的赋值看作相同, 则基域 $\mathbb{Q}$ 有一个唯一的阿基米德赋值 $\varphi(a) = |a|$, 此外, 对每个素数 p 有一个非阿基米德赋值, 即 p-adic 赋值：

$$\varphi_p(a) = p^{-m},$$

其中 m 是有理数 a 的因子分解中 p 的指数.

和阿基米德赋值相当的完备扩张就是实数域 $\mathbb{R}$. 再添加一个 i, 这个域就成为代数封闭的, 多项式 $F(x)$ 分解成一次因子：

$$F(x) = (x - \vartheta_1)(x - \vartheta_2) \cdots (x - \vartheta_n).$$

为了得出实的分解, 我们将两个相互共轭的复因子合并成一个实的二次式：

$$(x - a - bi)(x - a + bi) = (x - a)^2 + b^2.$$

设 r_1 是实根的个数, r_2 是共轭复根对的个数, 则 $F(x)$ 分解成 $r_1 + r_2$ 个实不可约因子.

相应于每个这样的因子有 Λ 的一个赋值, 只要用一个将 ϑ 映成实或复根 ϑ_ν 的同构将 Λ 嵌入到实或复数域中去, 就可得出这个相应的赋值来, 但在两个共轭的复根中每次只要取其中一个就行了. 这个同构将 ϑ 的每个函数

$$\eta = g(\vartheta) = c_0 + c_1\vartheta + \cdots + c_{n-1}\vartheta^{n-1}$$

映成 ϑ_ν 的相应的函数

$$\eta_\nu = g(\vartheta_\nu) = c_0 + c_1\vartheta_\nu + \cdots + c_{n-1}\vartheta_\nu^{n-1}.$$

因此, 相应的阿基米德赋值是

$$\Phi(\eta) = |\eta_\nu|.$$

这就是说：η 的 $r_1 + r_2$ 个阿基米德赋值由与 η 共轭的实数与复数 η_ν 的绝对值给出, 这里从两个共轭复数中只取其一.

代数数域的 $r_1 + r_2$ 个阿基米德赋值和域中的可逆元素有着十分密切的关系. 参看 van der Waerden B L. *Abh. Math. Sem. Hamburg*, 1928, 6: 259.

p-adic 赋值的研究可以完全类似地进行. 相应于 $\mathbb{Q}$ 的赋值 $\varphi=\varphi_p$ 的完备域即 p-adic 数域 Ω_p. 我们在 Ω_p 中将 $F(x)$ 分解成不可约因子：

$$F(x)=F_1(x)F_2(x)\cdots F_s(x). \tag{18.19}$$

对每个不可约多项式 F_ν, 我们将它的一个零点 ϑ_ν 添加到 Ω_p 上, 并作出相应的同构将 $\eta=g(\vartheta)$ 映成 $\eta_\nu=g(\vartheta_\nu)(\nu=1,\cdots,s)$. 由这一同构即得出赋值

$$\varPhi_\nu(\eta)=\varPhi(\eta_\nu)=\sqrt[n_\nu]{\varphi_p(N_\nu(\eta_\nu))}, \tag{18.20}$$

或取对数

$$W_\nu(\eta)=\frac{1}{n_\nu}w_p(N_\nu(\eta_\nu)). \tag{18.21}$$

这里的范数 $N_\nu(\eta_\nu)$ 就是 η_ν 的全部共轭元素的乘积, 只要在 $\eta_\nu=g(\vartheta_\nu)$ 中将 ϑ_ν 依次换成多项式 $F_\nu(x)$ 的全部根, 就可以得出这些共轭元素来. 设 $F_\nu(x)$ 的根是 $\vartheta_{\nu1},\vartheta_{\nu2},\cdots$, 则

$$N_\nu(\eta_\nu)=g(\vartheta_{\nu1})\cdot g(\vartheta_{\nu2})\cdots \tag{18.22}$$

是根 $\vartheta_{\nu1},\vartheta_{\nu2},\cdots$ 的一个对称函数, 因而可由 F_ν 的系数表出. 这样, 只要知道了分解式 (18.19), 我们就可以利用公式 (18.21) 找出所有的赋值 $W_\nu(\eta)$ 来.

例　试定出二次域 $\varLambda=\mathbb{Q}(\sqrt{5})$ 的全部赋值.

以 $\vartheta=\sqrt{5}$ 为零点的定义多项式是

$$F(x)=x^2-5.$$

在实数域中 $F(x)$ 分解成两个实的一次因子

$$F(x)=(x-\sqrt{5})(x+\sqrt{5}).$$

因此, 当我们把 ϑ 映成 $-\sqrt{5}$ 或 $\sqrt{5}$ 时, 可能得到两种不同的嵌入. 设

$$\eta=a+b\vartheta$$

为任意的域元素, 则相应的赋值是

$$\varphi_0(\eta)=|a+b\sqrt{5}| \tag{18.23}$$

和

$$\varphi_1(\eta)=|a-b\sqrt{5}|. \tag{18.24}$$

这样我们就把两个阿基米德赋值找出来了. 现在让我们来考虑 p-adic 赋值.

$F(x)$ 的判别式等于 20. 我们暂把能整除判别式的两个素数 2 和 5 除外.

对所有其余的素数 p 来说, $F(x)$ 模 p 无重因子. 因此只可能出现两种情况：或者 $F(x)$ 模 p 不可约, 或者 $F(x)$ 模 P 分解成两个一次因子. 如果一个因子是 $x-c$, 则另一因子是 $x+c$, 因为 x^2-5 的两个零点之和必等于零. 因此, 在第二种情形下, 我们有

$$\begin{aligned} &x^2-5 \equiv (x-c)(x+c) \pmod p, \\ &5 \equiv c^2 \pmod p. \end{aligned} \tag{18.25}$$

这就是说, 存在一个整数 c, 其平方模 p 同余于 5. 我们也说, 5 是一个模 p 二次剩余.

反之, 如果 $c^2 \equiv 5(p)$, 则分解式 (18.25) 成立. 因此, 如果 5 不是一个模 p 二次剩余, 则 x^5-5 模 p 不可约; 如果 5 是二次剩余, 则 x^2-5 模 p 分解成两个一次因子.

在第一种情形下 $F(x)$ 也是 p-adic 不可约的; 在第二种情形下, 根据 Hensel 引理, $F(x)$ 在 Ω_p 中可分解成两个一次因子.

根据前面所述, 在第一种情形下相应于素数 p 只有一个赋值

$$\Phi(\eta) = \sqrt{\varphi_p(N(\eta))}.$$

再一次命

$$\eta = a + b\vartheta = a + b\sqrt{5},$$

则有

$$N(\eta) = (a+b\sqrt{5})(a-b\sqrt{5}) = a^2-5b^2.$$

因此, 对所有使得 5 不是二次剩余的素数 p 来说,

$$\Phi(\eta) = \sqrt{\varphi_p(a^2-5b^2)}. \tag{18.26}$$

对于使得 5 是二次剩余的素数 p, 根据 Hensel 引理, 我们有 p-adic 分解

$$x^2-5 = (x-\gamma)(x+\gamma). \tag{18.27}$$

p-adic 数 γ 可以用下面的办法求出：解同余式

$$c^2 \equiv 5,$$

先对模 p 求解, 再对模 p^2 求解, 余此类推. 每次都可以得到两个解 c 和 $-c$. 这样, 我们就得到以 $p, p^2, \cdots$ 为模的两个同余类序列, 在每个序列中每个同余类包含在前一个同余类之内. 其中一个序列决定 γ, 另一序列决定 $-\gamma$.

最后, 为了得到 $\mathbb{Q}$ 的 p-adic 赋值 φ_p 的两个开拓, 只要将代数数域的生成元 ϑ 一次映射成 γ, 一次映射成 $-\gamma$ 即可. 如命

$$\eta = a + b\vartheta,$$

则所要求的两个赋值就是

$$\Phi_1(\eta) = \varphi_p(a + b\gamma), \tag{18.28}$$

$$\Phi_2(\eta) = \varphi_p(a - b\gamma), \tag{18.29}$$

由于 Ω_p 的 p-adic 赋值 φ_p 是已知的, 故 Φ_1 和 Φ_2 也就随之完全确定.

还可以指出, 在具体的情况下, 并没有必要将模 $p, p^2, \cdots$ 的无限多个同余类全部计算出来, 经过有限多步之后就可以中断这一过程. 事实上, 决定赋值 $\varphi_p(a+b\gamma)$ 时, 起决定作用的是 p-adic 数 $a + b\gamma$ 能被 p 的怎样一个幂整除. 举例来说, 如果经过三步之后可以断定它能被 p^2 整除, 而不能被 p^3 整除, 则

$$\varphi_p(a + b\gamma) = p^{-2}.$$

余下来需要讨论的, 是判别式的两个素因子 $p = 2$ 和 $p = 5$.

根据 Eisenstein 准则 (习题 18.11), $F(x) = x^2 - 5$ 在 Ω_5 中是不可约的, 因为在这个多项式中, 除头一个系数之外, 所有系数都能被 5 整除, 而最末一个系数不能被 5^2 整除. 因此 (18.26) 对 $p = 5$ 也成立.

在 Ω_2 中 Eisenstein 准则不再适用. 可是, 如果我们命 $x = 2y + 1$, 则有

$$x^2 - 5 = (2y + 1)^2 - 5 = 4(y^2 + y - 1),$$

而 $y^2 + y - 1$ 模 2 不可约. 因此 $x^2 - 5$ 是 2-adic 不可约的, (18.26) 对 $p = 2$ 也成立.

习题 18.15 多项式 $x^2 + 1$ 在实数域和域 Ω_2 中都不可约. 以某一奇素数 p 为模的多项式是否可约视 $p = 4k + 1$ 或 $p = 4k - 1$ 而定 (同余类域 $GF(p)$ 的乘法群是一个 $(p - 1)$ 阶巡回群. 它是否包含四次单位根, 视 $(p - 1)$ 能否被 4 除尽而定).

习题 18.16 试确定 Gauss 数 $a + bi$ 所成的域的全部赋值. 一共有多少个阿基米德赋值? 对怎样的 p 有两个赋值, 对怎样的 p 只有一个赋值?

我们在 18.1 节看到了经典理想论与赋值论之间的密切联系. 现在可以对这个关系作进一步的阐述.

仍设 $\mathbb{Z}$ 是有理数域 $\mathbb{Q}$ 里的整数环, 且设 $\mathfrak{o}$ 是代数数域 Λ 内的整量构成的环. 由 17.3 节, 我们有包含关系

$$\begin{array}{ccc} \mathbb{Z} & \subseteq & \mathfrak{o} \\ \cap & & \cap \\ \mathbb{Q} & \subseteq & \Lambda \end{array}$$

先写出指数赋值. 考虑 Λ 的赋值 W, 它是 $\mathbb{Q}$ 的 p-adic 赋值 w_p 的延拓. w_p 的定义如下：如果整数 m 恰好被 p^r 整除, 整数 n 恰好被 p^s 整除, 则

$$w_p\left(\frac{m}{n}\right) = r - s.$$

我们先证明以下断言.

对 $\mathfrak{o}$ 的元 a, $W(a)$ 非负.

假定 $W(a)$ 是负的. 作为整元, a 满足方程

$$a^n = c_1 a^{n-1} + \cdots + c_n, \tag{18.30}$$

其中 c_i 是 $\mathbb{Z}$ 的元素. (18.30) 的左边的值

$$W(a^n) = nW(a)$$

是负的, 而右边则取更大的值. 导出矛盾.

$\mathfrak{o}$ 里满足 $W(a) > 0$ 的 a 的集合是 $\mathfrak{o}$ 里的素理想 $\mathfrak{p}$. 设 π 是 $\mathfrak{o}$ 内恰好被 $\mathfrak{p}$ 的一次幂整除的元素. 如果 a 恰好被 $\mathfrak{p}^r$ 整除, 则根据 17.4 节,

$$a\mathfrak{o} = \mathfrak{p}^r \mathfrak{c}. \tag{18.31}$$

在 $\mathfrak{c}$ 中存在一个不被 $\mathfrak{p}$ 整除的元素 c. 由 (18.31), $\pi^r c$ 被 a 整除：

$$\pi^r c = ab. \tag{18.32}$$

由于左边恰好被 $\mathfrak{p}^r$ 整除, 而右边的因子 a 也是如此, 因此 b 不被 $\mathfrak{p}$ 整除, 从而 $W(b) = 0$. 同理有 $W(c) = 0$. 由 (18.32) 得

$$W(a) = W(\pi^r) = rW(\pi). \tag{18.33}$$

由于 $W(\pi)$ 是一个正常数, 赋值 W 等价于 $\mathfrak{p}$-adic 赋值

$$W_{\mathfrak{p}}(a) = r. \tag{18.34}$$

这样就得到了以下主要结果：

Λ 的所有非阿基米德赋值等价于由环 $\mathfrak{o}$ 的素理想 $\mathfrak{p}$ 定义的 $\mathfrak{p}$-adic 赋值. $\mathfrak{o}$ 的每个非零真素理想 $\mathfrak{p}$ 对应一族等价的非阿基米德赋值 W, 而且反过来也对.

由于赋值 W 在 $\mathbb{Q}$ 上等同于 p-adic 赋值 w_p, 所以在 W 下素数 p 取值 1. 现在把 (18.33) 应用于 $a = p$. 左边等于 1, 右边的 r 不能取零值. 这蕴含素理想 $\mathfrak{p}$ 必须出现在以下因式分解式的右边

$$(p) = p\mathfrak{o} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}, \tag{18.35}$$

设为 $\mathfrak{p}=\mathfrak{p}_\nu$. 这样在 (18.33) 的右边可令 $r=e_\nu$, 可得

$$1=e_\nu W(\pi).$$

如果在 (18.33) 的两边乘以 e_ν, 从 (18.34) 可得

$$e_\nu W(a)=W_{\mathfrak{p}}(a), \tag{18.36}$$

或者表述成：为了从赋值 $W(a)$ 得到规范化的 $\mathfrak{p}$-adic 赋值 $W_{\mathfrak{p}}(a)$, 必须把 $W(a)$ 的值乘以指数 e_ν, 这里 $\mathfrak{p}=\mathfrak{p}_\nu$ 是 (18.35) 中出现的素理想.

(18.35) 右边出现的不同素理想个数 s 等于域 $\mathbb{Q}$ 的 p-adic 赋值 w_p 的不同延拓的个数. 它也等于 (18.19) 右边的素因子个数, 在那里也记为 s.

整元的判则　域 Λ 的元 a 属于环 $\mathfrak{o}$ 的充分必要条件是 a 在域 Λ 的所有 $\mathfrak{p}$-adic 赋值里都取非负值.

我们已经证明了必要性. 现在设 $a=\dfrac{b}{c}$ 是 Λ 的元, 其中 b 和 c 都属于 $\mathfrak{o}$. 我们对主理想 (b) 和 (c) 作分解

$$(b)=\mathfrak{p}_1^{r_1}\cdots\mathfrak{p}_m^{r_m}, \tag{18.37}$$

$$(c)=\mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_m^{s_m}. \tag{18.38}$$

必要时插入因子 $\mathfrak{p}^0$, 可以假设 (18.37) 和 (18.38) 里出现同样的素理想 $\mathfrak{p}_\nu$. 关于素理想 $\mathfrak{p}_\nu$ 的 $\mathfrak{p}$-adic 赋值 $W_\nu(a)$ 的值为

$$W_\nu(a)=r_\nu-s_\nu.$$

如果所有这些值都是正数或零, 那么理想 (b) 被 (c) 整除. 由此可得

$$b=cd,$$

从而 $a=\dfrac{b}{c}=d$ 属于 $\mathfrak{o}$, 证毕.

刚才证明的定理可以重新叙述为:

定理　环 $\mathfrak{o}$ 是商域 Λ 所有 $\mathfrak{p}$-adic 赋值的赋值环的交, 这里的 $\mathfrak{p}$ 取遍除 $(0),(1)$ 外的所有素理想.

类似的定理对于任意在商域里整闭的整环都对 (参见 Krull W. Idealtheorie. *Ergebn. Math.*, Vol. 4 Heft 3).

18.7　有理函数域 $\Delta(x)$ 的赋值

任意一个域 Δ(“常数” 域) 都可以添加一个不定元 x 而得有理函数域 $\Delta(x)$. 我们要找出有理函数域 $\Delta(x)$ 的那样一些赋值, 在这些赋值中 Δ 中, 所有非零常数具有值 1.

特别, 在这样的赋值中所有和 $1+1+\cdots+1$ 有值 1. 因此, 这种赋值是非阿基米德赋值. 如果把它表成指数形式

$$\varphi = e^{-w},$$

则对所有常数 a, 有 $w(a)=0$.

可能出现两种不同的情况：

(1) 对所有多项式 $f(x), w(f) \geqslant 0$;

(2) 存在一个多项式 $f(x)$, 使得 $w(f)<0$.

可能对所有多项式 f 都有 $w(f)=0$. 在这一情形下所有的商 f/g 也都有值 0, 所考虑的赋值是平凡的.

除去这一情况外, 在第一种情形下存在一个多项式 f, 使得 $w(f)>0$. 如果将 f 分解成素因子, 那么至少有一个素因子的值 >0; 仍为 0.

设这个素因子是 $p(x)$, 而其值为 $v=w(p)$, 则每个不能被 $p(x)$ 整除的多项式的值都为零. 事实上, 设 $q(x)$ 是一个不能被 $p(x)$ 整除的多项式, 而其值 >0, 那么由于 p 和 q 互素, 故有

$$1 = Ap + Bq,$$

其中 A 和 B 都是多项式. 由此即可得

$$w(Ap) = w(A) + w(p) > 0,$$

$$w(Bp) = w(B) + w(q) > 0,$$

因而据非阿基米德赋值的基本性质有

$$w(1) = w(Ap+Bq) > 0,$$

而这是不可能的.

设 $f(x)$ 是一个任意的多项式, 并命

$$f(x) = p(x)^m q(x),$$

其中 $q(x)$ 不再能被 $p(x)$ 整除, 则 $f(x)$ 的值立即可以得出

$$w(f) = mw(p) + w(q) = mv.$$

对于多项式的商, 像通常一样有

$$w\left(\frac{f}{g}\right) = w(f) - w(g).$$

因此, 在第一种情形下所考虑的赋值等价于由一个素多项式 $p = p(x)$ 所定义的 p-adic 赋值. 这种赋值和有理数域的 p-adic 赋值完全相似.

特别简单的情形是常数域 Δ 为一代数封闭域的情形. 这时除了一次式

$$p(x) = x - a$$

之外不再有其他的素多项式.

相应于 Δ 中的每个 a, 恰有一个素多项式 $p = x - a$, 因而也恰有一个 p-adic 赋值. 当我们把 a 看作是一个复平面上的一个点时, 这个赋值称为属于点 a 的赋值. 如果一个多项式恰被 $(x-a)^m$ 整除, 或者说, 这个多项式以 a 为它的 m 阶零点, 那么在这个赋值下多项式的值是 m. 如果一个有理函数 $\varphi = f/g$ 的分子能被 $(x-a)^m$ 整除, 而分母不能被 $x - a$ 整除, 它的值也是 m. 如果情况恰恰与此相反, 则 φ 以 a 为它的一个 "m 阶极点", 而 φ 的值 $w(\varphi)$ 是 $-m$.

这样, 第一种情形就完全解决了. 现在我们要证明, *在第二种情况下, 除等价赋值外只有唯一的一个赋值, 即*

$$w\left(\frac{f}{g}\right) = -m + n,$$

其中 m 为分子 f 的次数, 而 n 为分母 g 的次数.

证　设 $p(x)$ 是使得 $w(p) < 0$ 的一个次数最低的多项式. $p(x)$ 的次数不可能为零, 因为根据我们的假设, 所有常数都有值零. 另一方面, $p(x)$ 的次数也不可能大于 1. 事实上, 如果

$$p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \quad n > 1, a \neq 0,$$

则多项式 x 的次数较 $p(x)$ 的次数为低, 因而有值 $w(x) \geqslant 0$, 从而多项式 a_0x^n 也具有一个 $\geqslant 0$ 的值. 另一方面, 多项式 $a_1x^{n-1} + \cdots + a_n$ 的次数也低于 $p(x)$ 的次数, 故其值也是 $\geqslant 0$ 的. 这样一来, 和

$$p(x) = ax^n + (a_1x^{n-1} + \cdots + a_n)$$

的值也 $\geqslant 0$, 而这是与所设相违的. 因此, $p(x)$ 是一次多项式:

$$p(x) = x - c.$$

现设

$$q(x) = x - b = (x - c) + (c - b)$$

为另一个一次多项式, 则由于 $w(x - c) < w(c - b)$, 故根据早些时候所作过的一个注记, 应有

$$w(q) = \min(w(x - c), w(c - b)) = w(p).$$

这就是说, 所有的一次多项式都具有同一负值 $w(p) = w(q) = -v$.

我们总可以由所考虑的赋值过渡到一个等价的赋值, 使得 $v = 1$. 这时所有一次多项式都有值 -1.

所有的幂 x^k 都具有值 $-k$, 乘上一个常数因子之后也不会改变它们的值, 因此

$$w(ax^k) = -k.$$

最后, 每个多项式 f 都是一些形为 ax^k 的项的和. 根据前面所作过的注记, f 的值 $w(f)$ 应等于各个项之值的最小者. 如 f 的次数为 n, 则

$$w(f) = -n,$$

这就证明了我们的定理.

在有理数域的情形, 一个阿基米德赋值和无限多个 p-adic 赋值之间存在着重大的差别. 在有理函数域的情形, 按次数的赋值和 p-adic 赋值却是属于同一性质的. 说得更确切些, 通过一个非常简单的域同构可把按次数的赋值转变为任意 p-adic 赋值. 事实上, 如命

$$x = \frac{1}{y-c}, \tag{18.39}$$

则次数为 m 和 n 的两个多项式的商

$$\varphi(x) = \frac{f(x)}{g(x)} = \frac{ax^m + \cdots}{bx^n + \cdots}$$

经过代换 (18.39), 并将分子分母都乘以 $(y-c)^{m+n}$ 之后, 就成为 y 的两个多项式的商, 其分子可被 $(y-c)^n$ 整除, 分母可被 $(y-c)^m$ 整除. 在属于点 c 的赋值中, 商 $\psi(y)$ 的值是 $n-m$. 这样, 同构 (18.39) 就把域 $\Delta(x)$ 的按次数的赋值转变成为同构域 $\Delta(y)$ 的属于点 c 的赋值.

由 (18.39) 可以看出, 和 "点"$y = c$ 相对应的是 "点"$x = \infty$. 因此我们说, 按次数的赋值是函数域 $\Delta(x)$ 的属于点 ∞ 的赋值. 复平面添加一个点 ∞ 之后即成为球面, 而在球面上所有的点都是同等的. 分式线性变换

$$y = \frac{ax+b}{cx+d} \tag{18.40}$$

将球面上的每个点变成每个另外的点. (18.39) 显然是 (18.40) 的一个特例.

现在我们问: 相应于域的不同的 "位", 能够作出怎样一些完备域来. 早些时候 (18.2 节) 我们已经看到, 和 $p = x - c$ 相应的完备域, 即所有形式幂级数

$$\alpha = a_{-m}(x-c)^{-m} + \cdots + a_0 + a_1(x-c) + a_2(x-c)^2 + \cdots$$

所成的域. 幂级数的系数为完全任意的常数. 不论系数如何选择, 幂级数在 p-adic 赋值的意义下是收敛的. 当 c 为复数时, 幂级数在函数论的意义下不一定收敛：收敛半径完全可能等于零.

如果 a_{-m} 是上面所写出的幂级数中第一个不为零的系数, 则这个幂级数的值 $w(\alpha)$ 等于 $-m$.

与此完全类似, 和点 $x=\infty$ 相应的完备域即 x^{-1} 的所有幂级数

$$\beta = b_{-m}x^m + \cdots + b_0 + b_1x^{-1} + b_2x^{-2} + \cdots$$

所成的域.

18.8 逼 近 定 理

像以前所指出, 对 K 的每一赋值 φ, 就有一极限概念：$\lim a_\nu = a$ 表示 $\lim\varphi(a_\nu - a) = 0$. 我们直接可证：

$$\lim \frac{a_\nu}{1+a_\nu} \begin{cases} = 0, & \text{当 } \varphi(a) < 1, \\ = 1, & \text{当 } \varphi(a) > 1. \end{cases}$$

两个这种赋值 φ 与 ψ, 若从 $\lim\varphi(a_\nu) = 0$, 总可得到 $\lim\psi(a_\nu) = 0$, 而且反过来也成立, 则 φ 与 ψ 等价.

在 18.2 节已经证明了以下的等价性判则.

引理 1 两个赋值 φ 与 ψ, 若从 $\varphi(a) < 1$ 可得 $\psi(a) < 1$, 则 φ 与 ψ 等价.

下面再证明第二个引理.

引理 2 设 $\varphi_1, \cdots, \varphi_n (n > 1)$ 为域 K 上有限个不等价的赋值. 于是存在域元素 a, 使

$$\varphi_1(a) > 1 \quad \text{且 } \varphi_\nu(a) < 1 \quad (\nu = 2, \cdots, n).$$

我们对 n 用归纳法来证明, 首先设 $n = 2$. 这里赋值 φ_1 与 φ_2 不等价. 按引理 1, 存在元素 b, 具有性质：

$$\varphi_1(b) < 1 \quad \text{且 } \varphi_2(b) \geqslant 1,$$

又有元素 c, 具有性质：

$$\varphi_1(c) \geqslant 1 \quad \text{且 } \varphi_2(c) < 1.$$

于是 $a = b^{-1}c$ 就具有所需的性质：

$$\varphi_1(a) > 1 \quad \text{且 } \varphi_2(a) < 1.$$

现设这定理对 $n-1$ 个赋值是对的, 于是存在元素 b, 使

$$\varphi_1(b)>1 \ \text{且}\ \varphi_\nu(b)<1 \quad (\nu=2,\cdots,n-1).$$

由 $n=2$ 时已证得的结果, 还存在元素 c, 使

$$\varphi_1(c)>1 \ \text{且}\ \varphi_n(c)<1.$$

分两种情况来讨论.

情况 1 $\varphi_n(b)\leqslant 1$. 作 $a_r=cb^r$. 于是

$$\varphi_1(a_r)>1,\quad \varphi_n(a_r)<1,$$

且对充分大的 r,

$$\varphi_\nu(a_r)<1\quad (\nu=2,\cdots,n-1).$$

因此可以取 $a=a_r$.

情况 2 $\varphi_n(b)>1$. 作

$$d_r=\frac{cb^r}{1+b^r}.$$

序列 $\{d_r\}$ 在赋值 φ_1 与 φ_n 下收敛于 c, 在其余的赋值 φ_ν 下收敛于 0. 因此

$$\begin{aligned}&\lim\varphi_1(d_r)=\varphi_1(c)>1,\\&\lim\varphi_n(d_r)=\varphi_n(c)<1,\\&\lim\varphi_\nu(d_r)=0\quad(\nu=2,\cdots,n-1).\end{aligned}$$

于是对充分大的 $r, a=d_r$ 就有所需的性质:

$$\begin{matrix}\varphi_1(a)>1,\\ \varphi_\nu(a)<1\end{matrix}\qquad (\nu=2,\cdots,n). \tag{18.41}$$

引理 3 设 $\varphi_1,\cdots,\varphi_n$ 为互不等价的赋值, 则存在域元素 b, 在赋值 φ_1 下任意接近于 1, 而在赋值 $\varphi_2,\cdots,\varphi_n$ 下任意接近于 0.

证 $n=1$ 的情形是显然的. 对 $n>1$ 的情形, 取一个具有性质 (18.41) 的元素 a. 再作

$$b_r=\frac{a^r}{1+a^r}.$$

序列 $\{b_r\}$ 在赋值 φ_1 下趋向于 1, 而在赋值 $\varphi_2,\cdots,\varphi_n$ 下趋向于 0. 于是就推得这个引理.

有了这些准备之后, 现在我们来证

逼近定理 设 $\varphi_1, \cdots, \varphi_n$ 为互不等价的赋值. 对给定的域元素 $a_1, \cdots, a_n$, 存在域元素 a, 它在赋值 φ_ν 下任意接近 a_ν:

$$\varphi_\nu(a_\nu - a) < \varepsilon \quad (\nu = 1, \cdots, n). \tag{18.42}$$

证 由引理 3, 存在元素 $b_\nu(\nu = 1, \cdots, n)$, 它在赋值 φ_ν 下任意接近 1, 而在所有其余赋值下任意接近于 0. 于是, 和

$$a = a_1 b_1 + \cdots + a_n b_n$$

在赋值 φ_ν 下任意接近 a_ν.

这里给出的逼近定理的证明取自 Artin 的讲演.

第 19 章　单变量代数函数

复数域上的代数函数古典理论以有了 Riemann-Roch 定理而达到高峰. 对这个定理有函数论的、几何的和代数的证明方法. 在 Jordan 所著《分析教程 II》(*Cours d'Analyse* II) 的第 8 章中可以找到运用几何思想的函数论证明方法的一个美好表述. 在几何证法方面, Severi 的快速方法① 特别值得提出. 由 Dedekind 和 Weber 所给出的纯代数的证明方法 (*J. Reine Angew. Math.*, 1882, 92) 被 Emmy Noether 所简化, 而且推广到完全的常数域上. 对于任意常数域, 首先由 Schmidt 给出了 Riemann-Roch 定理的证明 (*Math. Z.*, 1936, 41. 那里还有更多的文献). André Weil 在*J. Reine Angew. Math.*, 1938, 179 中给出了较简单的证明. 下面我们遵循他的证明.

19.1　按局部单值化元的级数展开

设 K 为单变量代数函数域, 即有理函数域 $\Delta(x)$ 的有限扩张. 独立变量 x 的选择有相当任意性：可以任选对 Δ 为超越的元素来代替 x. 我们感兴趣的只是不变量, 即不依赖于 x 的选择的代数函数域的性质.

K 中对 Δ 为代数的元素称为常量, 它们形成常量域 Δ^*. 域 Δ^* 在 K 中是代数闭的, 即 K 中对 Δ^* 为代数的元素一定在 Δ^* 中.

目前的代数函数化的出发点是赋值概念. 如同 18.7 节, 我们只考虑函数域 K 的使 $\varphi(c^*)=1$ 的赋值, 这里 c^* 是 Δ^* 的非零常数. 据 18.7 节, 可以直接看出, 所有这些赋值都是非阿基米德的. 把它们写成指数形式

$$\varphi(z)=e^{-w(z)}, \tag{19.1}$$

其中对 Δ^* 中的 $c^*\neq 0$ 有 $w(c^*)=0$.

习题 19.1　若对 Δ 的所有 $c\neq 0$, 有 $w(c)=0$, 则对 Δ^* 的所有 $c^*\neq 0$, 有 $w(c^*)=0$.

域 K 的位就是等价赋值的一个类. 只要审视 18.7 节以复数为常数域的有理函数域 $\Delta(x)$, 就能理解为什么称为 “位” 了. 如果向复数平面添一个点 ∞ 并想象成一个球面, 且把其上的每个点称为位, 那么每个位 (c 或 ∞) 恰好对应一个等价赋值类. 根据 18.7 节, 有理函数域 $\Delta(x)$ 的所有赋值都能如此得到.

---

① 这个方法的最新表达可参考*Severi F. Acta Pont. Accad. sci.*, 1952. Weil 的证明也受到快速方法的影响, 这个证明将在这里表述出.

对于复数域上的代数函数域, 考虑这个函数域的 Riemann 面[①], 也能应用类似的方法. 在 18.1 节证明了, 这个曲面的每个点 P 对应这个函数域 K 的一个等价赋值类. 在这个情形也可以证明[②], 所有在常数 c 上取 $w(c)=0$ 的赋值都能用这种方式得到.

本书后面关于位与单值化元的理论将以纯代数的形式展开, 不涉及 Riemann 面. 当在讨论中谈到 "位" 的时候, 读者不妨把它想象成 Riemann 面的一个点.

对于函数域 K 的每个位, 也就是说, 等价赋值的类, 在 18.1 节已经对应了赋值环 $\mathfrak{J}$ 以及赋值理想 $\mathfrak{p}$, 后者由满足 $w(z)>0$ 的域元素 z 构成. 由 18.8 节的引理 1, 属于同一个赋值理想 $\mathfrak{p}$ 的赋值是等价的. 因此每个赋值理想对应一个位. 以后用同样的字母 $\mathfrak{p}$ 记这个位.

根据假设, 域 K 是有理函数域 $\Delta(x)$ 的有限扩域. K 的所有赋值可用如下方法得到：先按 18.7 节找出 $\Delta(x)$ 的所有赋值, 然后如 18.5 节所述, 通过用所有可能的方式把 K 嵌入到多项式 $F(t)$ 在完备域 Ω 上的分裂域 Λ 中, 以把上述赋值扩张到 K. K 的指数赋值 w 可以先扩张成 Ω 的同类赋值 w. 根据 18.4 节, 然后可将它唯一扩张成 Λ 的赋值 W, 使得对 Λ 的每个元素 z 有

$$\Phi(z)=\sqrt[m]{\varphi(N(z))},$$

或者回到指数赋值 w 与 W,

$$W(z)=\frac{1}{m}w(N_\Lambda(z)),$$

其中 m 是 Λ 在 Ω 上的域扩张次数. 对于每个已知的赋值 w, 只可能有有限多个开拓 W. 在经典理论里的相应事实是：球面上每个点的上方存在着函数域 K 的 Riemann 面的有限多个点.

按 18.7 节, $\Delta(x)$ 的赋值 w 是离散的, 即存在一个最小正值 w_0, 所有值 $w(z)$ 都是 w_0 的倍数. 因此 K 的赋值 W 也是离散的.

如前, 我们把赋值 $W(z)$ 规范化一下, 使 $W(z)$ 的最小正值取作 1. 于是所有的 $W(z)$ 都是整数. 这样规范化了的赋值只依赖于位 $\mathfrak{p}$, 记作 $W_\mathfrak{p}$, 或简记为 $\mathfrak{p}$. 对每一个位有一局部单值化元 π, 具有 $W_\mathfrak{p}(\pi)=1$. 整数 $W_\mathfrak{p}(z)$ 称为*函数 z 在位 $\mathfrak{p}$ 处的阶*. 若 $W_\mathfrak{p}(z)=k$ 为正的, 则称 $\mathfrak{p}$ 是函数 z 的 *k 阶零位*, 或称为函数 z 的 *k重零位*. 若 $W_\mathfrak{p}(z)=-h$ 为负的, 则称 $\mathfrak{p}$ 为函数 z 的 *h 阶极位*, 或函数 z 的 *h 重极*.

按 18.1 节, 同余类环 $\bar{\mathfrak{J}}=\mathfrak{J}/\mathfrak{p}$ 总是域, 即赋值的剩余类域. 这个域总包含以 Δ^* 中元素 (常量) 作为代表元的那些同余类所成的域 $\bar{\Delta}^*$. 因为 $\bar{\Delta}^*$ 与 Δ^* 是同构的,

① 参见 Weyl H. *Die Idee der Riemannschen Flache*, 3. Aufl., Teubner, Stuttgart, 1955.
② 证明可见 *Algebra*, Vol. I. 4. to 6. Aufl., pp. 280–282.

所以我们可以把 $\bar{\Delta}^*$ 与 Δ^* 等同起来, 因而可以把 $\bar{\mathfrak{J}}$ 看成 Δ^* 的扩域. 常量域 Δ^* 仍然是基本域 Δ 的扩域.

现在我们证明, $\bar{\mathfrak{J}}$ 是 Δ 的有限扩域.

证　因为 π 不属于 Δ^*, 所以 π 对 Δ 是超越的, 于是 K 对 $\Delta(\pi)$ 是代数的. K 由 $\Delta(\pi)$ 通过添加有限多个元素而成, 所以 K 对 $\Delta(\pi)$ 也是有限的. 设 K 对 $\Delta(\pi)$ 的次数为 m.

现在设 $\bar{\mathfrak{J}}$ 中有 $m+1$ 个对 Δ 线性无关的同余类 $\bar{\omega}_1,\cdots,\bar{\omega}_{m+1}$. 相应地, 在这些同余类中取 $\mathfrak{J}$ 中元素 $\omega_1,\cdots,\omega_{m+1}$. 这 $m+1$ 个元素对 $\Delta(\pi)$ 必须是线性相关的. 于是有

$$f_1(\pi)\omega_1+\cdots+f_{m+1}(\pi)\omega_{m+1}=0, \tag{19.2}$$

其中 $f_1(\pi),\cdots,f_{m+1}(\pi)$ 是 $\Delta(\pi)$ 中的多项式, 且不全为零. 我们可以取得使它们不全为 π 所整除. 在模 $\mathfrak{p}$ 下, 分别相应地取它们的常数项 $c_1,\cdots,c_{m+1}$. 于是由 (19.2) 得

$$c_1\omega_1+\cdots+c_{m+1}\omega_{m+1}\equiv 0(\mathfrak{p}),$$

或即

$$c_1\bar{\omega}_1+\cdots+c_{m+1}\bar{\omega}_{m+1}=0.$$

这样就与 $\bar{\omega}_i$ 是线性无关的假设矛盾. 因此 $\bar{\mathfrak{J}}$ 对 Δ 的次数最多为 m.

这就证明了 $\bar{\mathfrak{J}}$ 对 Δ 是有限的. 因为 Δ^* 是 $\bar{\mathfrak{J}}$ 的子域, 所以 Δ^* 对 Δ 也是有限的. 若 Δ 是代数闭的, 则 $\bar{\mathfrak{J}}=\Delta^*=\Delta$.

从现在起, 我们不再把 Δ 作为基本域而把 Δ^* 作为基本域, 而且不再加星号. 也就是把 Δ 看成在 K 中是代数闭的.

以后把 $\bar{\mathfrak{J}}$ 对 Δ 的次数用 $f_{\mathfrak{p}}$ 表示, 或简单地用 f 来表示. 对于代数闭的常量域的典型情形, 当然 $f=1$.

我们现在把域 K 的元素 z 按局部单值化元 π 展开成幂级数. 令 $(\bar{\omega}_1,\cdots,\bar{\omega}_f)$ 是 $\bar{\mathfrak{J}}$ 对于 Δ 的一组基, ω_i 是同余类 $\bar{\omega}_i$ 中任一元素. 设 z 是一个阶为 b 的元素, 则 $z\pi^{-b}$ 是一个阶为 0 的元素, 因而属于 $\bar{\mathfrak{J}}$. 所以模 $\mathfrak{p}$ 的同余式

$$z\pi^{-b}\equiv c_1\omega_1+\cdots+c_f\omega_f(\mathfrak{p}) \tag{19.3}$$

成立, 其中系数 $c_i\in\Delta$ 是唯一确定的. 差

$$z\pi^{-b}-(c_1\omega_1+\cdots+c_f\omega_f) \tag{19.4}$$

是 $\mathfrak{p}$ 中的元素, 因而是 π 的倍元:

$$z\pi^{-b}=c_1\omega_1+\cdots+c_f\omega_f+z'\pi,$$
$$z=(c_1\omega_1+\cdots+c_f\omega_f)\pi^b+z'\pi^{b+1}.$$

余项 $z_1 = z'\pi^{b+1}$ 至少是 $b+1$ 阶的, 于是可以对 z' 重复同样过程. 在 s 步后, 得到

$$z = \sum_{k=b}^{b+s-1} (c_{k1}\omega_1 + \cdots + c_{kf}\omega_f)\pi^k + z_s,$$

其中余项 z_s 至少是 $b+s$ 阶.

令 $s \to \infty$, 余项 z_s 趋于极限零, 从而得到

$$z = \sum_{k=b}^{\infty} (c_{k1}\omega_1 + \cdots + c_{kf}\omega_f)\pi^k, \tag{19.5}$$

其中系数 $c_{ki} \in \Delta$ 都是唯一确定的. 开始项的指数 b 可以是负的, 但是在级数 (19.5) 中出现的负指数项只能是有限项.

我们可以把这个过程稍许改进一下, 取阶为 b 的任意元素 π_b 代替 π^b, 并且从 (19.3) 式写出 $z\pi_b^{-1}$ 的同余式. 于是代替 (19.5), 我们有关于 π_k 的级数展开:

$$z = \sum_{k=b}^{\infty} (c_{k1}\omega_1 + \cdots + c_{kf}\omega_f)\pi_k. \tag{19.6}$$

在 (19.6) 式中, π_k 是任意的, 只需取阶为 k 的函数即可. 系数 c_{ki} 是 Δ 的唯一确定的元素.

在 18.8 节中所证的逼近定理, 现在对函数域来说可以表述如下:

定理 1 若对有限多个位任意给出级数 (19.5) 的有限截断, 那么总可以有域 K 中的函数 z, 使得 z 在这些位上的级数展开各取所给的有限截断作为它们的开始项.

我们称这个定理为独立定理. 进一步有

定理 2 一个非常量函数 z 只有有限个零位和极.

证 域 K 的每一赋值 W 总是域 $\Delta(z)$ 的某一赋值 w 的开拓. $\Delta(z)$ 只有两个位使 z 有正的或负的阶, 即位 $z=0$ 和 $z=\infty$. 也只有属于这两个位的赋值 w 才能使 $w(z) \neq 0$. 每一个这种赋值只有有限个方法开拓为 K 的赋值 W. 因此只有有限个 K 的位使 $W(z) \neq 0$.

用同样的方法我们可以得出, 每一个非常量函数至少有一个零位及一个极. 实际上, $\Delta(z)$ 的属于位 $z=0$ 或 ∞ 的赋值至少有一种方法开拓为 K 的赋值. 因此有

定理 3 没有极的函数是常量.

级数展开 (19.5) 和 (19.6) 不仅对域 K 的元素成立, 而且对完备化的域 Ω_K 的元素也成立. 设 z 是 Ω_K 中的元素, b 为 z 的阶, 于是 $z\pi^{-b}$ 是零阶元素. 这样的元素可以用 $\mathfrak{J}$ 中元素 y 任意逼近, 即可以逼近到具有任意高阶的误差. 在我们这里的

情形, 只要求逼近到 1 阶误差就可以了. 对于这个元素 y, 仍然有同余式

$$y \equiv c_1\omega_1 + \cdots + c_f\omega_f(\mathfrak{p}).$$

差 $y-(c_1\omega_1+\cdots+c_f\omega_f)$ 可以被 π 整除, 又因为差 $z\pi^{-b}-y$ 也可以被 π 整除, 所以这两个差的和 (即 (19.4) 式) 是 π 的倍元, 从而也可以像前面一样地进行.

19.2　除子及其倍元

仍设 K 是对于常量域 Δ 的单变量代数函数域. K 中函数仍然只用字母 u,v,w,x,y,z,ϑ 和 π 来表示.

带有任意整指数 d 的有限个位 $\mathfrak{p}$ 定义域 K 的一个除子 D. 我们形式地将 D 写成有限个因子的乘积

$$D=\prod \mathfrak{p}^d. \tag{19.7}$$

这个乘积的因子允许任意交换. 当指数 d 是零的时候, 可以在 D 中把因子 p^d 去掉. 如果所有 d 都是零, 则 $D=(1)$ 称为单位除子. 如果所有 $d\geqslant 0$, 则称 D 为整除子.

两个除子的相乘，就把相同因子 $\mathfrak{p}$ 的指数相加. 对每一个具有指数 d 的除子 D, 有一个具有指数 $-d$ 的逆除子 D^{-1}, 使 $D^{-1}D=(1)$. 除子做成一个交换群, 称为域 K 的除子群. 单独一个位 $\mathfrak{p}$ 也称为素除子. 它们生成除子群.

每一个函数 z 决定一个除子

$$(z)=\prod \mathfrak{p}^d,$$

其中指数 d 等于 z 在位 $\mathfrak{p}$ 处的阶. 常量 z 总对应于单位除子. 乘积 yz 对应于除子 (y) 与 (z) 的乘积：

$$(yz)=(y)(z).$$

素除子 $\mathfrak{p}$ 的次数, 即同余类域 $\bar{\mathfrak{J}}=\mathfrak{J}/\mathfrak{p}$ 对域 Δ 的次数, 像 19.1 节一样, 仍以 f 记之. 在 (19.7) 中出现的因子的次数的和

$$n(D)=\sum df$$

叫做除子 D 的次数.

把 $(z)D$ 简单地写成 zD. 当 zD^{-1} 是整除子时, 称函数 z 为除子 D 的倍元, 这就是说, 对域 K 的所有位 $\mathfrak{p}$ 有

$$W_{\mathfrak{p}}(z)\geqslant d. \tag{19.8}$$

除子 D 的倍元就是这种函数 z, 它对一切具有指数 $d=h>0$ 的位, 至少有一个 h 重零位, 对一切具有指数 $d=-k<0$ 的位至多有一个 k 重极, 对所有其余的位保持有限, 即不是极.

一个除子 A^{-1} 的倍元形成一个 Δ 模, 以 $\mathfrak{M}(A)$ 表示. 我们现在证明, $\mathfrak{M}(A)$ 对于 Δ 是有限秩的.

设 $A=\prod \mathfrak{p}^a$. 因为在乘积中只出现有限个具有 $a>0$ 的因子 $\mathfrak{p}^a$, 所以总只有有限多个位 $\mathfrak{p}$, 它是 A^{-1} 的倍元 z 的极. 如果以前的 ω_i 现在用 w_i 表示, z 在这些位的级数展开可以表成

$$z=(c_{-a,1}w_1+\cdots+c_{-a,f}w_f)\pi^{-a}+\cdots.$$

对于一个位 $\mathfrak{p}$, 属于负幂 $\pi^{-a},\cdots,\pi^{-1}$ 的系数 $c_{-i,j}$ 的个数是 af, 对于所有这种极位总共就是

$$m=\sum af,$$

这里对所有具 $a>0$ 的位 $\mathfrak{p}$ 求和. 我们要证不可能有多于 $m+1$ 个 A^{-1} 的线性无关的倍元 z.

假如有 $m+2$ 个这样的倍元 $z_1,\cdots,z_{m+2}$, 我们可以做常系数的线性组合

$$z=b_1z_1+\cdots+b_{m+2}z_{m+2}, \tag{19.9}$$

并且限定在 z 的展开式中负幂的系数全部是零. z 的这个条件是对 $m+2$ 个系数 $b_1,\cdots,b_{m+2}$ 的 m 个线性条件. 每一个对系数 b_i 的线性条件都促使函数 (19.9) 所成的模的秩最多降低 1, 因此, 满足线性条件 $c_{-i,j}=0$ 的函数所成的模的秩至少是 $(m+2)-m=2$. 这些函数 z 都没有极, 因此按 19.1 节定理 3, 都是常量, 但常量所成的模对于 Δ 的秩是 1, 所以除子 A^{-1} 最多只能有 $m+1$ 个线性无关的倍元, 即 $\mathfrak{M}(A)$ 的秩最多为 $m+1$.

下面讨论的目的是决定 $\mathfrak{M}(A)$ 的秩 $l(A)$, 也就是除子 A^{-1} 的线性无关的倍元的个数. 我们也把 $l(A)$ 叫做 A 的维数. 上面所给的证明中, 对整除子 A 给出了不等式

$$l(A)\leqslant n(A)+1. \tag{19.10}$$

若 AB^{-1} 是整除子, 则称除子 $A=\prod \mathfrak{p}^a$ 能被除子 $B=\prod \mathfrak{p}^b$ 所整除, 即对所有 $\mathfrak{p}, a\geqslant b$. 显然, 此时有

$$n(A)\geqslant n(B)\quad 且 l(A)\geqslant l(B).$$

我们将导出差 $n(A)-l(A)$ 的一个不等式, 方法和上面是一样的. A^{-1} 的倍元是

$$z=b_1z_1+\cdots+b_lz_l,\tag{19.11}$$

其中 b_i 是常量, $l=l(A)$. 要使函数 z 不仅属于 $\mathfrak{M}(A)$ 而且也属于 $\mathfrak{M}(B)$, 必须在展开式

$$z=(c_{-a,1}w_1+\cdots+c_{-a,f}w_f)\pi^{-a}+\cdots$$

中, 幂 $\pi^{-a},\pi^{-a+1},\cdots,\pi^{-b-1}$ 的系数都是零. 这样对每一个位给出了 $(a-b)f$ 个线性方程, 总共对 (19.11) 中系数 $b_1,\cdots,b_l$ 给出了

$$\sum(a-b)f=\sum af-\sum bf=n(A)-n(B)$$

个线性方程. 每一个线性方程至少使秩降低 1, 这就给出了

$$l(B)\geqslant l(A)-[n(A)-n(B)]$$

或

$$n(A)-l(A)\geqslant n(B)-l(B).\tag{19.12}$$

当 B 能整除 A 时, (19.12) 式总成立. 特别取 A 为一个整除子, $B=(1)$, 则 (19.12) 的右端等于

$$0-1=-1,$$

又重新得到了 (19.10) 式.

下面的定理几乎是自明的:

定理　*若 $z\neq 0$, 则 $\mathfrak{M}(A)$ 与 $\mathfrak{M}(zA)$ 有相同的秩:*

$$l(A)=l(zA).$$

证　设 $y_1,\cdots,y_l$ 为 $(zA)^{-1}=z^{-1}A^{-1}$ 的线性无关的倍元, 则

$$y_1z,\cdots,y_lz$$

是 A^{-1} 的线性无关的倍元, 反之也对.

两个仅差一个因子 (z) 的除子 A 与 zA 叫做等价的. 于是有: *等价的除子有相同的维数.*

习题 19.2　设 $A=\prod\mathfrak{p}^a$ 是有理函数域 $K=\Delta(x)$ 中的一个除子. 证明: A^{-1} 的倍元将由

$$z=f(x)\prod p(x)^{-a}$$

给出, 其中 $p(x)$ 为素多项式, 按 18.7 节, 它属于在 A 中出现而不等于 $\mathfrak{p}_\infty$ 的素除子 $\mathfrak{p}$.

习题 19.3　在习题 19.2 的基础上证明:

$$l(A)=n(A)+1,\quad 当\ n(A)\geqslant 0,$$
$$l(A)=0,\quad 当\ n(A)<0.$$

19.3 亏　　格

设 z 为域 K 的一个非常量函数. 除子 (z) 可以表成两个没有公共素因子 $\mathfrak{p}$ 的整除子的商:

$$(z)=CD^{-1}. \tag{19.13}$$

C 叫做 z 的**分子除子**, D 叫做 z 的**分母除子**. 设 K 对 $\Delta(z)$ 的次数为 n. $C=\prod\mathfrak{p}^c$ 的次数是

$$n(C)=\sum cf,$$

对于 D 有相应的等式.

现在我们证明重要等式

$$n(C)=n(D)=n. \tag{19.14}$$

我们用 $\mathfrak{p},\mathfrak{p}',\cdots$ 表示 $C=\prod\mathfrak{p}^c$ 的素因子, 它们的指数用 $c,c',\cdots$ 表示. 域 K 中一个对 $\mathfrak{p}$ 为整的函数 u 在位 $\mathfrak{p}$ 处有展开式

$$u=\sum_0^\infty(a_{k1}w_1+\cdots+a_{kf}w_f)\pi^k. \tag{19.15}$$

我们把 π^{c-1} 以后的项丢掉, 写成

$$u\equiv\sum_{k=0}^{c-1}\sum_{i=0}^{f}a_{ki}w_i\pi^k \pmod{\pi^c}, \tag{19.16}$$

相应地, 对于其他的位 $\mathfrak{p}'$ 等有同样的式子.

按独立定理 1(19.1 节), 存在 $c\cdot f$ 个函数 u_{ki}, 它们在位 $\mathfrak{p}$ 处的始截断 (19.16) 只是 $w_i\pi^k$ 而在其他位 $\mathfrak{p}',\cdots$ 处的始截断都是零. 同样存在 $c'f'$ 个函数 u'_{ki}, 它们在位 $\mathfrak{p}'$ 处的始截断为 $w'_i\pi'^k$, 等等. 现在我们可证:

$cf+c'f'+\cdots=n(c)$ 个函数 $u_{ki},u'_{ki},\cdots$ 对 $\Delta(z)$ 是线性无关的.

假设有线性关系

$$\sum f_{ki}(z)u_{ki}+\sum f'_{ki}(z)u'_{ki}+\cdots=0, \tag{19.17}$$

其中 $f_{ki}, f'_{ki}, \cdots$ 为 z 的多项式. 我们可以取这些函数使它们的常数项 $c_{ki}, c'_{ki}, \cdots$ 不全为零. 在 (19.17) 式中, 以 $u_{ki}, u'_{ki}, \cdots$ 在位 $\mathfrak{p}$ 处的级数展开 (19.15) 和 z 在 $\mathfrak{p}$ 处的展开式代入, 再像 (19.16) 那样取模 π^c 计算, 于是 $f_{ki}(z)$ 化为它的常数项 c_{ki}, u_{ki} 化为 $w_i\pi^k$, 而其余的 u'_{ki} 变为零. 于是从 (19.17) 得到

$$\sum_{k=0}^{c-1}\sum_{i=1}^{f} c_{ki}w_i\pi^k \equiv 0(\pi^c).$$

由于级数展开式 (19.15) 的唯一性, 只可能所有的 $c_{ki} = 0$. 同样得到所有的 $c'_{ki} = 0$ 等等. 这样就导致矛盾.

由上面所证的线性无关性得

$$n \geqslant n(C).$$

处处以 z^{-1} 代替 z, 我们就同样可证

$$n \geqslant n(D).$$

设 $(u_1, \cdots, u_n)$ 为 K 关于 $\Delta(z)$ 的一组基. 我们总可以如此选取, 使得 u_j 在所有使 z 有限的位上都是有限的. 事实上, 如果 u_j 有一个极位 $\mathfrak{p}$, 在 $\mathfrak{p}$ 上 z 是有限的, 那么有一个属于这个极位的赋值 $W_{\mathfrak{p}}$, 它也诱导出域 $\Delta(z)$ 的一个赋值, 而且不是属于位 $z = \infty$ 的赋值 W_∞. 按 18.7 节, 域 $\Delta(z)$ 的不同于 W_∞ 的赋值都是 p-adic 赋值, 即属于素多项式 $p = p(z)$, 这里 p 在所讨论的位上有正的阶. 对足够大的 d, 乘积 $p^d u_j$ 在 $\mathfrak{p}$ 上不再是极. 于是我们可以把 u_j 的所有使 z 为有限的极位逐个地取消, 在这里我们只是用适当的 z 的多项式去乘基元素 u_j.

z 的极都含在分母除子 D 中. 因此对于足够大的 m_i, u_i 是 D^{-m_i-1} 的倍元. 我们进一步选取 m 大于所有的 m_i:

$$m \geqslant m_i + 1 \quad (i = 1, \cdots, n).$$

$\sum(m - m_i)$ 个域元素

$$z^\mu u_i \quad (0 \leqslant \mu < m - m_i)$$

是对于 Δ 线性无关的, 而且是 D^{-m} 的倍元, 也就含于 $\mathfrak{M}(D^m)$ 中. 因此有

$$\sum(m - m_i) \leqslant l(D^m) \leqslant n(D^m) + 1$$

或

$$nm - \sum m_i \leqslant l(D^m) \leqslant m \cdot n(D) + 1. \tag{19.18}$$

令 m 趋于无穷, 于是由 (19.18) 得出

$$n \leqslant n(D).$$

又因为已经证明了 $n \geqslant n(D)$, 所以

$$n = n(D). \tag{19.19}$$

自然同样也有

$$n = n(C). \tag{19.20}$$

由 (19.19) 和 (19.20) 得

$$n((z)) = n(CD^{-1}) = 0. \tag{19.21}$$

由 (19.21) 又得到

$$n(zA) = n(A). \tag{19.22}$$

这就是说: 等价的除子不仅有相同的维数 $l(A)$, 而且也有相同的次数 $n(A)$.

把 (19.19) 代入 (19.18) 得

$$n(D) \cdot m - \sum m_i \leqslant l(D^m)$$

或

$$n(D^m) - l(D^m) \leqslant \sum m_i. \tag{19.23}$$

如果 B 是 D^m 的一个因子, 那么由 (19.12) 有

$$n(B) - l(B) \leqslant n(D^m) - l(D^m),$$

因此由 (19.23) 有

$$n(B) - l(B) \leqslant \sum m_i. \tag{19.24}$$

现在设 A 是任意一个除子. 我们要证 (19.24) 对 A 也成立. 为此只要证明, 存在一个与 A 等价的除子 $uA = B$, 它是幂 D^m 的一个因子.

设 $\mathfrak{p}$ 是在 $A = \prod \mathfrak{p}^d$ 中以正指数出现的一个素因子. 如果所有这种 $\mathfrak{p}$ 都是 z 的极位, 则 A 本身就是 D^m 的一个因子, 从而证毕. 若 $\mathfrak{p}$ 不是 z 的极位, 那么总可以找到一个多项式 $p = p(z)$, 它在位 $\mathfrak{p}$ 处有正的阶. 用 p^{-d} 乘 A, 就在 A 中消掉了因子 $\mathfrak{p}^d$. 重复这个过程, 可以把 A 中一切不属于 z 的极位并且具有 $d > 0$ 的因子 $\mathfrak{p}^d$ 消掉. 因此最后总可以找到一个与 A 等价并且是 D^m 的因子的除子 $B = uA$, (19.24) 对 B 来说成立, 从而也对 A 成立:

$$n(A) - l(A) \leqslant \sum m_i, \tag{19.25}$$

换句话说, 差 $n(A)-l(A)$ 对所有 A 来说是有界的.

对于所有除子 $A, n(A)-l(A)+1$ 的上确界 g 叫做域 K 的亏格.

对于 $A=(1), n(A)-l(A)=0-1=-1$, 所以 $g \geqslant 0$. 亏格 g 是一个非负整数, 它是函数域 K 的一个数值不变量.

按照亏格的定义, 对于一切 A 都有

$$n(A)-l(A)+1 \leqslant g$$

或

$$l(A) \geqslant n(A)-g+1, \tag{19.26}$$

这里至少有一个除子 A 使得等号成立. 不等式 (19.26) 常称为 Riemann-Roch 定理的 Riemann 部分.

令

$$l(A)=n(A)-g+1+i(A), \tag{19.27}$$

称 $i(A)$ 为除子 A 的特殊指数. 若 $i(A)>0$, 称 A 为特殊除子. 若 A 不是特殊的, 则 $n(A)-l(A)$ 取最大可能值 $g-1$. 非特殊的除子总是存在的. 我们的问题是, 确定特殊指数 $i(A)$, 然后证明完整的 Riemann-Roch 定理.

习题 19.4 有理函数域 $K=\Delta(z)$ 的亏格是 0 并且具有次数为 1 的素除子.

习题 19.5 若 K 的亏格是零且具有次数为 1 的素除子, 则 K 是一个有理函数域 $\Delta(z)$ (应用 (19.26) 式于 $A=\mathfrak{p}$).

19.4 向量与协向量

域 K 的函数在一个位 $\mathfrak{p}$ 处的级数展开中, 作为 π 的幂的系数出现的是

$$v=c_1 w_1+\cdots+c_f w_f. \tag{19.28}$$

这些表示式形成 (对于每一个位 $\mathfrak{p}$) Δ 上的一个 f 维向量空间 L_f.

我们可以把在位 $\mathfrak{p}$ 处的幂级数较简单地写成

$$V_{\mathfrak{p}}=\sum_a^{\infty} v_k \pi^k, \tag{19.29}$$

或者为了表达出系数 v_k 对于位 $\mathfrak{p}$ 的依赖性, 写成

$$V_{\mathfrak{p}}=\sum_a^{\infty} v_{\mathfrak{p} k} \pi^k. \tag{19.30}$$

如果对于每一个位 $\mathfrak{p}$, 有以 L_f 中元素 $v_{\mathfrak{p}k}$ 为系数的一个幂级数 (19.30) 与它对应, 而且在所有这些幂级数中总共只有有限项以负指数出现, 那么这个幂级数组就叫做一个**向量**V. 幂级数 $V_{\mathfrak{p}}$ 叫做向量 V 的**分量**. 从不依于局部单值化元 π 和 (19.28) 中基向量 w_i 的特殊选择的角度出发, 我们也可以把 $V_{\mathfrak{p}}$ 看成属于位 $\mathfrak{p}$ 的完备扩域 $\Omega_K(\mathfrak{p})$ 的元素. 对于这些元素 $V_{\mathfrak{p}}$, 只允许有有限个负的阶 $W_{\mathfrak{p}}(V_{\mathfrak{p}})$, 其他的选择是完全任意的.

若级数 (19.30) 在每一个位 $\mathfrak{p}$ 处都是从 π^d 开始:

$$w_{\mathfrak{p}}(V_{\mathfrak{p}}) \geqslant d, \quad \text{对一切 } \mathfrak{p},$$

则称向量 V 被除子 $D = \prod \mathfrak{p}^d$ 所整除.

特别地, 域 K 的函数 u 对应一个向量 V, 因为每一个函数 u 在每一个位 $\mathfrak{p}$ 处都有一个幂级数展开 (19.30), 而所有这些幂级数中总共只出现有限个具有负指数的项.

根据 4.3 节, 向量空间 L_f 有对偶向量空间 D_f, D_f 的元素是 L_f 上的线性函数.

对于 L_f 的元 $v = \sum c_i w_i$ 与 D_f 的 α, 可以构造数量积

$$v \cdot \alpha = c_1\alpha_1 + \cdots + c_f\alpha_f.$$

用类似方法, 我们现在对于由向量 V 所成的无限维空间 $\mathfrak{V}$, 作出由协向量构成的对偶空间.

对于每一个位 $\mathfrak{p}$, 令 D_f 中的一个元素序列 $\{\alpha_{\mathfrak{p}k}\}(k = b, b+1, \cdots)$ 与它对应, 在所有这些序列中总共只出现有限多个负指数 k, 则称这个序列组为一个**协向量** λ. 向量 V 与协向量 λ 的数量积定义为

$$V \cdot \lambda = \sum_{\mathfrak{p}} \sum_{i+k=-1} v_{\mathfrak{p}j} \cdot \alpha_{\mathfrak{p}k}. \tag{19.31}$$

因为只有有限多个 $v_{\mathfrak{p}j}$ 具有负的 j 并且只有有限多个 $\alpha_{\mathfrak{p}k}$ 具有负的 k, 所以和式 (19.31) 中只出现有限项. 每一个单项都是数量积 $v \cdot \alpha$, 从而是 Δ 的元素.

算子 $\cdot\lambda$ 是由向量 V 的空间 $\mathfrak{V}$ 到常量域内的映射, 它具有下列性质:

(A) $(V + W) \cdot \lambda = V \cdot \lambda + W \cdot \lambda$;

(B) $(cV) \cdot \lambda = c(V \cdot \lambda)$;

(C) $V \cdot \lambda = 0$, 当 V 能被只依赖于 λ 的某除子 D 所整除时.

(A) 与 (B) 是显然的. 为了证 (C), 我们注意, 只有有限多个 $\mathfrak{p}$ 使得序列 $\{\alpha_{\mathfrak{p}k}\}$ 以负指数 $k = -d$ 开始. 我们以带有指数 d 的这些个位 $\mathfrak{p}$ 作成除子

$$D = \prod \mathfrak{p}^d,$$

于是 (C) 成立.

所有能被 D 整除的向量 V 的全体, 可以看作向量空间 $\mathfrak{B}$ 里的零的邻域. 性质 (C) 表明, 线性泛函 λ 把 $\mathfrak{B}$ 的某一个零的邻域映成零. 因此性质 (C) 是一种连续性质.

我们现在证明:

每一个满足性质 (A)~(C) 的从 $\mathfrak{B}$ 到 Δ 上的映射 $\cdot\lambda$ 都可以用上述方法通过序列 $\{\alpha_{\mathfrak{p}k}\}$ 定出.

证　每一个向量 V 可以表成一个能被 D 整除的向量和有限个向量 $V_{\mathfrak{p}j}$ 的和, 这些 $V_{\mathfrak{p}j}$ 在位 $\mathfrak{p}$ 处的展开中只有一项 $v\pi^j$, 而其余的分量都是零:

$$(V_{\mathfrak{p}j})_{\mathfrak{p}} = v\pi^j,$$
$$(V_{\mathfrak{p}j'})_{\mathfrak{p}'} = 0, \quad \text{对}\mathfrak{p}' \neq \mathfrak{p}\text{或}j' \neq j.$$

这里 $v = \sum c_i w_i$ 是向量空间 L_f 的元素. 把映射 $\cdot\lambda$ 作用在上面所定义的向量 $V_{\mathfrak{p}_j}$ 上, 就得到 Δ 的元素 $V_{\mathfrak{p}j}\cdot\lambda$, 它线性地依赖于 v, 因此可以写成 $v\cdot\alpha$, 其中 α 为 D_f 中的元素. 我们把元素 α 记作 $\alpha_{\mathfrak{p}k}$, 其中 k 是由

$$j + k = -1$$

所决定的. 因为 $V_{\mathfrak{p}j}$ 不能被 D 整除, 所以 $j < d$, 从而 $k \geqslant -d$. 因此在序列 $\{\alpha_{\mathfrak{p}k}\}$ 中总共只出现有限多个负指数. 于是, 由 (A) 和 (C) 得

$$V\cdot\lambda = \sum_{\mathfrak{p}}\sum_{\mathrm{j}} V_{\mathfrak{p}j}\cdot\lambda = \sum_{\mathfrak{p}}\sum_{j+k=-1} v_{\mathfrak{p}j}\cdot\alpha_{\mathfrak{p}k},$$

证毕.

在这一定理的基础上, 我们也可以把协向量 λ 定义作为具有性质 (A)~(C) 的从 $\mathfrak{B}$ 到 Δ 内的映射. 这个定义具有不变性, 即不依赖于 w_i 和 π 的选取.

19.5　微分, 关于特殊指数的定理

现在利用协向量来决定特殊指数 $i(B)$. 首先证明两个引理:

若除子 D 不是特殊的且 A 是 D 的倍除子, 则 A 也不是特殊的.

证　按 (19.12),

$$n(A) - l(A) \geqslant n(D) - l(D).$$

由于 $n(D) - l(D)$ 已经取极大值 $g-1$, 所以 $n(A) - l(A)$ 也取极大值 $g-1$.

推论　*每一个除子 B 都有一个非特殊的倍除子 A.*

证　设 D 不是特殊的. 取 A 为 B 和 D 的公共倍除子. 由引理就直接得出这个推论.

现在设 $A = \prod \mathfrak{p}^a, B = \prod \mathfrak{p}^b$. 如果 A 是 B 的一个倍除子, 则 $b \leqslant a$ 且 $\mathfrak{M}(B) \subseteq \mathfrak{M}(A)$. 我们取 B 是特殊的, 而 A 不是特殊的. 于是有

$$l(A) = n(A) - g + 1, \tag{19.32}$$

$$l(B) = n(B) - g + 1 + i(B). \tag{19.33}$$

如同 19.2 节那样, 我们把 $\mathfrak{M}(A)$ 中元素

$$u = b_1 u_1 + \cdots + b_l u_l \tag{19.34}$$

属于 $\mathfrak{M}(B)$ 时所应当满足的 $\sum (a-b)f$ 个线性方程写出来. 如果 u 在位 $\mathfrak{p}$ 处的级数展开是这样开始的:

$$u = (c_{-a,1} w_1 + \cdots + c_{-a,f} w_f)\pi^{-a} + \cdots , \tag{19.35}$$

那么对于位 $\mathfrak{p}$ 的 $(a-b)f$ 个条件是

$$c_{j\nu} = 0 \quad (-a \leqslant j < b, 1 \leqslant \nu \leqslant f). \tag{19.36}$$

$c_{j\nu}$ 当然依赖于 $\mathfrak{p}$. 实际上应该写成 $c_{j\nu}(\mathfrak{p})$, 然而以后仍然把它省掉.

如果 $\sum (a-b)f = n(A) - n(B)$ 个方程 (19.36) 是独立的, 那么将有

$$l(A) - l(B) = n(A) - n(B).$$

然而, 由 (19.32) 和 (19.33), 差 $l(A)-l(B)$ 比 $n(A)-n(B)$ 小 $i(B)$, 所以方程 (19.36) 的左端存在 $i(B)$ 个线性关系, 这就是说, 对于 $\mathfrak{M}(A)$ 中每一元素 u, 必须满足 $i(B)$ 个线性无关的关系

$$R\{c_{j\nu}\} = \sum_{\mathfrak{p}} \sum_{j=-a}^{-b-1} \sum_{\nu=1}^{f} c_{j\nu}\gamma_{j\nu} = 0. \tag{19.37}$$

如果把对 f 的和理解作数量积:

$$\sum_1^f c_{j\nu}\gamma_{j\nu} = \nu_j \cdot \beta_j,$$

那么等式 (19.37) 还可以写得简单一些. 这里 $v_j = \sum c_{j\nu} w_\nu$, $\beta_j = \beta_j(\mathfrak{p})$ 是序列

$(\gamma_{j1},\cdots,\gamma_{if})$. 为了得到以前表达的结果. 令 $v_j = v_{\mathfrak{p}j}$ 及

$$\beta_j(\mathfrak{p}) = \alpha_{\mathfrak{p}k} \quad (j+k=-1).$$

于是 (19.37) 变成

$$R\{c_{j\nu}\} = \sum_{\mathfrak{p}} \sum_{j+k=-1} v_{\mathfrak{p}j}\cdot\alpha_{\mathfrak{p}k} = 0, \tag{19.38}$$

其中

$$b \leqslant k \leqslant a-1.$$

现在用 A 的倍除子

$$A' = \prod \mathfrak{p}^{a'} \quad (a' \geqslant a)$$

来代替 A. 于是得

$$\mathfrak{M}(B) \subseteq \mathfrak{M}(A) \subseteq \mathfrak{M}(A').$$

A' 作为 A 的倍除子, 也不是特殊的, 于是重新得到 $i(B)$ 个线性关系

$$R'\{c_{j\nu}\} = \sum_{\mathfrak{p}} \sum_{j+k=-1} v_{\mathfrak{p}j}\cdot\alpha'_{\mathfrak{p}k} = 0, \tag{19.39}$$

其中 $b \leqslant k \leqslant a'-1$. 这些关系对 $\mathfrak{M}(A')$ 中所有 u 都要满足.

关系 R, 或更确切地说, 系数组 $\{\alpha_{\mathfrak{p}k}\}$ 组成一个秩为 $i(B)$ 的 Δ 模. 同样, R' 组成一个秩为 $i(B)\Delta$ 模.

我们只要在关系 R' 中把 $k > a-1$ 的项丢掉, 就得到一个关系 R, 它被 $\mathfrak{M}(A)$ 中所有的 u 满足. 通过这个“射影”, 每一个 R' 给出一个 R, 映射 $R' \to R$ 是线性的. 如果 $R' \neq 0$ 而在射影下对应的 $R = 0$, 那么 R' 只有 $k > a-1$ 的项, 从而只有

$$-a' \leqslant j < -a$$

的项. 这一关系 R' 仍被 $\mathfrak{M}(A')$ 中一切元素 u 所满足. 我们再把 $\mathfrak{M}(A')$ 的元素属于 $\mathfrak{M}(A)$ 时所要满足的条件等式写出来, 那么条件 R' 就表示在这 $n(A')-n(A)$ 个条件等式中存在线性关系. 于是将有

$$l(A') - l(A) < n(A') - n(A),$$

这是不可能的, 因为 (19.32) 对 A' 和 A 都成立

因此映射 $R' \to R$ 是一对一的. 它把关系 R' 所成的模同构地映成关系 R 所成的模的一个子模, 这个子模的秩也是 $i(B)$, 因此, 它把 R' 所成的模同构地映成 R 所成的整个的模. 这就是说:

每一个关系 R 有唯一的方法开拓为关系 R'.

我们现在让 a 中的一个指数 a' 趋于无限而让关系 R 一直开拓下去, 于是我们得到唯一决定的无限序列

$$\{\alpha_{\mathfrak{p}k}\} \quad (k = b, b+1, \cdots). \tag{19.40}$$

我们可以对每一个位 $\mathfrak{p}$ 这样做. 于是对于一切位 $\mathfrak{p}$ 得到一组序列 (19.40), 即一个协向量. 现在关系 (19.39) 可以写成

$$u \cdot \lambda = 0. \tag{19.41}$$

关系 (19.41) 对 $\mathfrak{M}(A')$ 中一切元素 u 都成立. 然而我们可以对于域 K 的每一个函数 u 找一个除子 A', 它不仅能被 B 整除而且也能被 (u^{-1}) 整除. 于是 uA' 是整除子, 即 u 属于 $\mathfrak{M}(A')$, 从而 (19.41) 成立. 因此 (19.41) 对于域 K 的所有函数 u 都成立.

因为有 $i(B)$ 个线性无关的关系 R, 所以存在 $i(B)$ 个由 (19.40) 所定义的协向量 λ, 它们具有性质 (19.41). 我们给出定义 (按照 Weil):

定义 1 一个对于域 K 的所有 u 都有性质 (19.41) 的协向量 λ 叫做域 K 的一个微分.

Weil 的微分和古典函数论的微分的关系将在 19.8 节中说明.

定义 2 一个协向量 λ 叫做 $B = \prod \mathfrak{p}^b$ 的倍量, 如果在它的定义中只有 $k \geqslant b$ 的 $\alpha_{\mathfrak{p}k}$ 出现.

从协向量的定义直接得出: 对每一个协向量 λ 有一个除子 B, 使得 λ 是 B 的倍量.

在定义 1 和定义 2 的基础上, 我们可以将这一段中所证明的事实综述为:

特殊指数定理 特殊指数 $i(B)$ 等于作为 B 的倍量的线性无关的微分的个数.

定义 3 若微分 λ 是单位除子 (1) 的倍量, 则称 λ 是处处有限的或第一类微分, 这就是说, 具有负指数 k 的一切 $\alpha_{\mathfrak{p}k}$ 都是零.

为了得出线性无关的第一类微分的个数, 将特殊指数定理应用到除子 (1) 上, 公式 (19.27) 给出

$$\begin{aligned} i(1) &= l(1) - n(1) + g - 1 \\ &= 1 - 0 + g - 1 = g, \end{aligned}$$

于是, 线性无关的第一类微分的个数等于亏格 g .

如果取 $B = C^{-1}$, 其中 C 为 $\neq (1)$ 的一个整除子, 我们就得到特殊指数定理的另一个应用, 这时 $l(B) = 0$, 因为整除子 $B^{-1} = C$ 的唯一倍元是函数零. 其次,

$n(B)=-n(C)$, 所以

$$i(C^{-1})=n(C)+g-1. \tag{19.42}$$

特别, 取 $C=\mathfrak{p}^n$, 从而 $B=\mathfrak{p}^{-n}$, 于是 $n(C)=nf$, 我们得到

$$i(\mathfrak{p}^{-n})=nf+g-1. \tag{19.43}$$

于是有

定理　若 f 为素除子 $\mathfrak{p}$ 的次数, 那么存在 $nf+g-1$ 个线性无关的微分, 它们是 $\mathfrak{p}^{-n}$ 的倍元.

习题 19.6　设基域 Δ 是代数闭的. 那么除了第一类微分之外没有其他的作为 $\mathfrak{p}^{-1}$ 的倍量的微分, 即不存在只具有一个单极 $\mathfrak{p}$ 的微分.

习题 19.7　在同样假设下, 对于每个 $n>1$, 都存在一个第二类初等微分 $\omega(\mathfrak{p}^n)$, 它在 $\mathfrak{p}$ 处有一 n 重极. 每一个是 $\mathfrak{p}^{-n}$ 的倍量的微分都可以从 $\omega(\mathfrak{p}^2),\omega(\mathfrak{p}^3),\cdots,\omega(\mathfrak{p}^n)$ 和 g 个线性无关的第一类微分作线性组合而得到.

习题 19.8　在同样假设下, 对每两个位 $\mathfrak{p}_1$ 和 $\mathfrak{p}_2$ 存在一个第三类初等微分 $\omega(\mathfrak{p}_1,\mathfrak{p}_2)$, 它在 $\mathfrak{p}_1$ 和 $\mathfrak{p}_2$ 处都有单极. 每一个微分都可以从第二和第三类初等微分以及第一类微分作线性组合而得到.

19.6　Riemann-Roch 定理

我们现在即将达到目的. 首先我们定义一个函数 u 和一个协向量 λ 的乘积$u\lambda$. 这个乘积 $u\lambda$ 是作为 $\mathfrak{V}$ 到 Δ 内的线性映射而这样定义的：

$$V\cdot u\lambda=Vu\cdot\lambda. \tag{19.44}$$

算子 $\cdot u\lambda$ 显然具有 19.4 节中性质 (A)~(C), 所以由 (19.44) 定义了一个协向量 $u\lambda$.

如果 λ 是一个微分, 那么 $u\lambda$ 也是微分：

$$v\cdot u\lambda=vu\cdot\lambda=0,\quad \text{对一切 } v.$$

下面的引理几乎是自明的.

引理 1　若 λ 是除子 $D=\prod\mathfrak{p}^d$ 的倍量, 那么对于所有能被 D^{-1} 整除的向量 V, 都有 $V\cdot\lambda=0$; 反过来也成立.

证　设协向量 λ 由序列 $\{\alpha_{\mathfrak{p}k}\}$ 给出. 若 λ 是 D 的倍量, 则在序列中只有指数 $k\geqslant d$ 出现. 其次, 若 V 由幂级数

$$V_{\mathfrak{p}}=\sum v_{\mathfrak{p}j}\pi^j \tag{19.45}$$

给出, 并且 V 能被 D^{-1} 整除, 那么在幂级数 (19.45) 中只有 $j \geqslant -d$ 的项出现. 数量积

$$V \cdot \lambda = \sum_{\mathfrak{p}} \sum_{j+k=-1} v_{\mathfrak{p}j} \alpha_{\mathfrak{p}k} \tag{19.46}$$

等于零, 因为和 $j+k$ 总不能等于 -1. 反过来, 若对于所有能被 D^{-1} 整除的 V 都有 $V \cdot \lambda = 0$, 那么在序列 $\{\alpha_{\mathfrak{p}k}\}$ 中只能有 $k \geqslant d$ 的项出现, 于是 λ 是 D 的倍量.

引理 2 *若 λ 是 D 是倍量, 则 $u\lambda$ 是 uD 的倍量.*

证 由引理 1, 当 V 能被 D^{-1} 整除时, $V \cdot \lambda = 0$. 因此, 当 Vu 能被 D^{-1} 整除时, $Vu \cdot \lambda = 0$. 这就是说, 当 V 能被 $(uD)^{-1}$ 整除时, $V \cdot u\lambda = 0$.

现在设 λ 是一个微分. 由 19.5 节, 存在以 λ 为倍量的除子 D. 设 $B = \mathfrak{p}^{-n}$, 这里 $\mathfrak{p}$ 是次数为 f 的一个素除子. 除子 $B^{-1}D = \mathfrak{p}^n D$ 有次数

$$n(B^{-1}D) = nf + n(D).$$

根据 Riemann-Roch 定理的 Riemann 部分, BD^{-1} 的线性无关的倍元 u 的个数是

$$l(B^{-1}D) \geqslant nf + n(D) - g + 1. \tag{19.47}$$

若 u 是 BD^{-1} 的倍元, 那么 uD 是 B 的倍除子. 由引理 2, $u\lambda$ 是 uD 的倍量, 因此 $u\lambda$ 也是 B 的倍量. 但作为 B 的倍量的线性无关的微分的总数是 $i(B)$. 于是由 (19.47) 得

$$nf + n(D) - g + 1 \leqslant i(B). \tag{19.48}$$

按 (19.43), 对于 $n > 0$ 有

$$i(B) = nf + g - 1. \tag{19.49}$$

代入 (19.48) 得

$$n(D) \leqslant 2g - 2. \tag{19.50}$$

所以这种除子 D 的次数是有上界的. 因此, 对所给的微分 λ 有一极大除子 D_λ, 使得 λ 是 D_λ 的倍量, 而不管 $\mathfrak{p}'$ 怎么选取, λ 总不是 $D_{\lambda\mathfrak{p}'}$ 的倍量. 这个以 λ 为倍量的唯一确定的极大除子 D_λ 叫做*微分 λ 的除子*.

我们现在证明:

所有微分 ω 都等于 $u\lambda$, 这里 λ 是一个任意给定的微分.

证 假定有一个微分 ω, 它不等于 $u\lambda$. 于是得

$$u\lambda \neq v\omega \quad \text{对一切 } u \text{ 及 } v \neq 0. \tag{19.51}$$

如同在 (19.47) 中所见的一样, 至少有

$$nf+n(D_\lambda)-g+1$$

个线性无关的微分 $u\lambda$, 它们是 $B=\mathfrak{p}^{-n}$ 的倍量. 同样, 至少有

$$nf+n(D_\omega)-g+1$$

个线性无关的微分 $v\omega$, 它们是 B 的倍量. 所有这些微分是线性无关的, 因为没有 $u\lambda$ 的线性组合会等于 $v\omega$ 的线性组合. 于是总共有

$$2nf+\text{常数}$$

个线性无关的微分, 它们是 B 的倍量. 但根据 (19.49), 只有 $nf+g-1$ 个这样的微分. 对于充分大的 n, 这是一个矛盾. 因此正如命题所述, 所有微分都等于 $u\lambda$.

现在我们以任意一个除子 A 来代替 B, 并且重新提出, 有多少线性无关的微分 $\omega=u\lambda$, 它们是 A 的倍量. 若 $u\lambda$ 是 A 的倍量, 则 λ 是 $u^{-1}A$ 的倍量, 于是极大除子 D_λ 可以被 $u^{-1}A$ 整除, 从而 uD_λ 可以被 A 整除, u 可以被 AD_λ^{-1} 整除. 反之, 若 u 可以被 AD_λ^{-1} 整除, 则 $u\lambda$ 是 A 的倍量, 因为上述一切论断都可以倒过来. 这样就得到

$$i(A)=l(A^{-1}D_\lambda). \tag{19.52}$$

把这个等式代入 (19.27) 里, 就得到下述的完全的定理:

Riemann-Roch 定理 *设 A 是域 K 的任一除子, λ 是任一非零微分, 则有*

$$l(A)=n(A)-g+1+l(A^{-1}D_\lambda). \tag{19.53}$$

在这里还有一些补充.

(1) 令 $A=(1)$, 则由 (19.52) 或 (19.53) 得出

$$l(D_\lambda)=g. \tag{19.54}$$

(2) 令 $A=D_\lambda$, 则由 (19.53) 得出

$$n(D_\lambda)=2g-2. \tag{19.55}$$

(3) 若 λ 是 D 的倍量, 则 $u\lambda$ 是 uD 的倍量; 反过来也对. 若 D_λ 是微分 λ 的除子, 则 uD_λ 是微分 $u\lambda$ 的除子. 因此, 微分 $\omega=u\lambda$ 的除子 $D_\omega=uD_\lambda$ 都是彼此等价的. 这些除子 D_ω 的等价类叫做*微分类*或*典范类*.

(4) 一般地, 一个除子类是由等价于某一个除子 A 的所有除子 uA 所组成. 类中所有除子 uA 都有相同的维数 $l(A)$ 和相同的次数 $n(A)$. 因此可以称 $l(A)$ 为这个类的维数, 称 $n(A)$ 为这个类的次数.

类 $\{A\}$ 的维数还可以用下列方法表述. 若 u 可以被 A^{-1} 整除, 则 uA 是一个整除子. 于是模 $\mathfrak{M}(A)$ 中的元素 u 对应类 $\{A\}$ 中的整除子 uA. 若 $u_1, \cdots, u_r$ 线性无关, 那么就称除子 $u_1A, \cdots, u_rA$ 也线性无关. 于是模 $\mathfrak{M}(A)$ 的秩 $l(A)$ 就是类 $\{A\}$ 中线性无关的整除子的极大个数.

(5) 若 $n(A) < 0$, 则没有与 A 等价的整除子, 因而 $l(A) = 0$.

(6) 若 $n(A) > 2g - 2$, 则 $n(A^{-1}D_\lambda) < 0$, 于是由 (5) 有 $l(A^{-1}D_\lambda) = 0$. 由 (19.52) 就得出 $i(A) = 0$, 所以

具有 $n(A) > 2g - 2$ 的除子 A 不是特殊的.

习题 19.9 只有一个类 $\{A\}$ 具有 $l(A) \geqslant g$ 及 $n(A) = 2g - 2$, 这就是典范类.

习题 19.10 具有 $l(B) > g$ 的整除子不是特殊的.

对于任意基域 Δ 上的一般理论的建立到此就结束了. 我们现在将要转入古典的理论, 在那里 Δ 是复数域. 为此我们首先需要掌握一些有关可分性的知识.

一般的 Riemann-Roch 定理也可以转移到体上, 它是有理函数域 $\Delta(z)$ 的有限扩体. 可参看 Witt E. Riemann-Rochscher Satz und ζ-Funktion im Hyperkomplexen. *Math. Ann.,* 1934, 110: 12.

19.7 函数域的可分生成元

r 个变量的代数函数域 K 是 r 个代数无关元素 $x_1, \cdots, x_r$ 的有理函数域 $\Delta(x_1, \cdots, x_r)$ 的一个有限扩域.

设域 K 是由 $\Delta(x_1, \cdots, x_r)$ 通过添加 $x_{r+1}, \cdots, x_n$ 而生成的, 则

$$K = \Delta(x_1, \cdots, x_r, x_{r+1}, \cdots, x_n),$$

这里一切 x_i 都是独立变量 $x_1, \cdots, x_r$ 的代数函数.

对于这样的函数域来说, 以下的关于可分生成元的定理成立:

可分生成定理 *若常量域 Δ 是完全的, 那么总可以对 $x_1, \cdots, x_r$ 如此编号, 使得一切 x_i 都是独立变量 $x_1, \cdots, x_r$ 的可分代数函数.*

证 对于给定的 r, 我们对 n 作数学归纳法. 在 $u = r$ 的情形是显然的. 假定 $n > r$ 并且命题对于 $\Delta(x_1, \cdots, x_{n-1})$ 正确. 于是我们可以取 $x_1, \cdots, x_{n-1}$ 都是 $x_1, \cdots, x_r$ 的可分函数.

x_n 总是 $x_1, \cdots, x_r$ 的一个代数函数, 它满足方程

$$f(x_1, \cdots, x_r, x_n) = 0, \tag{19.56}$$

这个方程可以取得对一切 x_i 都是有理整的. 如果将域元素 $x_1, \cdots, x_r$ 和 x_n 用不定元 $X_1, \cdots, X_r$ 和 X_n 来代替, 则 $f(X_1, \cdots, X_r, X_n)$ 作为 X_n 的多项式是不可约的. 如果 f 作为 $X_1, \cdots, X_r, X_n$ 的多项式是可分解的, 那么将得到一个只含 $X_1, \cdots, X_r$ 的因子. 这样一个因子总可以从方程 (19.56) 中去掉. 因此, 可以假定 f 作为 $X_1, \cdots, X_r, X_n$ 的多项式也是不可约的.

若 x_n 对于 $\Delta(x_1, \cdots, x_r)$ 是可分的, 那就没有什么可证的了. 若 x_n 是不可分的, 那么域的特征是一个素数 p, 并且多项式 f 只含 X_n 的这样的幂, 它们可以写成 X_n^p 的幂. 如果在 f 中出现的 $X_1, \cdots, X_r$ 的幂也是这样, 那么

$$f = \sum a_s X_1^{ps_1} \cdots X_r^{ps_r} X_n^{ps_n}. \tag{19.57}$$

然而, 在完全域 Δ 里, 每一个 a_s 都是一个 p 次幂:

$$a_s = b_s^p.$$

因此

$$f = \left(\sum b_s X_1^{s_1} \cdots X_r^{s_r} X_n^{s_n}\right)^p.$$

但这是不可能的, 因为 f 是不可约的. 因此, 在变量 $X_1, \cdots, X_r$ 中至少有一个, 例如 X_1, 它在 f 中至少有一个不能被 p 整除的幂出现.

由 (19.56) 得出, x_1 是 $x_2, \cdots, x_r$ 及 x_n 的一个可分代数函数. 一切 x_i 都与 $x_1, \cdots, x_r$ 代数相关, 从而也与 $x_n, x_2, \cdots, x_r$ 代数相关. 因为 $\Delta(x_1, \cdots, x_n)$ 的超越次数等于 r, 所以 $x_n, x_2, \cdots, x_r$ 代数无关. 域 $\Delta(x_1, \cdots, x_n)$ 对于域 $\Delta(x_1, \cdots, x_r)$ 是可分的, 从而也对于 $\Delta(x_n, x_2, \cdots, x_r)$ 是可分的, 因此一切 x_i 对于 $\Delta(x_n, x_2, \cdots, x_r)$ 是可分的. 重新排列 x_i 的下标, 在这里只要把 1 和 n 对调一下, 就得到这个命题.

对于非完全域, Weil 给出了一个有可分生成元的充分与必要条件. 可参看 van der Waerden B L. Über Weils Neubegründung der Algebr. Geometrie. *Abh. Math. Sem., Hamburg*, 1958, 22: 158.

19.8 古典情形下的微分和积分

古典函数论考虑 Abel 积分

$$\int w dz,$$

这里 z 是一个独立变量, 亦即一个非常量函数, 而 w 是域 K 的任意一个函数. 对另一变量 t 的代换由公式

$$\int w dz = \int w \frac{dz}{dt} dt$$

实现.

在代数理论中我们可以去掉积分符号而只考虑 Abel 微分 wdz. 由一个变量 z 转变到另一个变量 t 时微分按公式

$$wdz = w\frac{dz}{dt}dt$$

转变.

然而, 在这里要使 dz/dt 有意义, 必须假设 z 对于 $\Delta(t)$ 是可分的 (参看 10.5 节). 因此, 我们有目的地限于这样的 t, 对它来说域 K 对于 $\Delta(t)$ 是可分的. 当域 K 有可分生成元的时候, 这样的 t 是存在的. 特别, 当 Δ 是完全的时候, 这样的 t 总存在.

为了简单起见, 总假定常量域 Δ 是代数闭的. 读者可以作为练习, 把这里的理论推广到任意的完全常量域上.

变量 z 总是这样选取, 使得 K 对于 $\Delta(z)$ 是可分的. 为了研究微分 wdz 在一位 $\mathfrak{p}$ 处的情况, 我们对这个位选取一个局部单值化元 π, 并且把 z 展成幂级数

$$z = P(\pi) = \sum c_k \pi^k. \tag{19.58}$$

当用幂级数 $P(\pi)$ 代入 z 时, 联系着 π 与 z 的不可约方程 $F(z,\pi)=0$ 被满足：

$$F(P(\pi),\pi) = 0. \tag{19.59}$$

方程左端是 π 的幂级数, 它的所有系数都要等于零. 对这个幂级数形式地取微商时, 它们仍然是零, 在这里幂级数 $P(\pi)$ 的形式的微商是由

$$P'(\pi) = \sum k c_k \pi^{k-1}$$

所定义. 若在 (19.59) 中当 $P(\pi)$ 仍以 z 代回去时, F 对 z 和 π 的偏微商分别以 F'_z 和 F'_π 表示, 就得到

$$F'_z(z,\pi)\cdot P'(\pi) + F'_\pi(z,\pi) = 0. \tag{19.60}$$

因为 π 对于 $\Delta(z)$ 是可分的, 所以 $F'_\pi(z,\pi)\neq 0$. 由 (19.60), $F'_z(z,\pi)$ 不能是零, 从而 z 对于 $\Delta(\pi)$ 是可分的. 于是微商 $dz/d\pi$ 有定义并且满足方程

$$F'_z(z,\pi)\cdot\frac{dz}{d\pi} + F'_\pi(z,\pi) = 0. \tag{19.61}$$

比较 (19.60) 与 (19.61) 得

$$\frac{dz}{d\pi} = P'(\pi) = \sum k c_k \pi^{k-1}. \tag{19.62}$$

于是可分变量 z 可以对每一局部单值化元求微商, 并且微商的幂级数是通过对 z 的幂级数逐项求微商而得到的.

现在微分 wdz 可以用局部单值化元 π 表达出来：

$$wdz = w\frac{dz}{d\pi}d\pi. \tag{19.63}$$

$w\dfrac{dz}{d\pi}$ 的幂级数自然通过 w 的幂级数与幂级数 (19.62) 相乘而得出. 设结果是

$$w\frac{dz}{d\pi} = \sum \alpha_{\mathfrak{p}k}\pi^k. \tag{19.64}$$

如果在级数 (19.64) 中没有负指数项出现, 那么就说微分 wdz 在位 $\mathfrak{p}$ 处是有限的. 如果只有大于 a 的指数带有非零系数出现, 那么就称 $\mathfrak{p}$ 是微分的一个 a 阶零位. 如果有负指数出现, 就称 $\mathfrak{p}$ 是微分的一个极, 微分在位 $\mathfrak{p}$ 处的阶指的是具有非零系数 $\alpha_{\mathfrak{p}k}$ 的最小指数 k. 所有这些概念显然与局部单值化元 π 的选择无关.

微分 wdz 的极应在 w 的极和 z 的极中间去找, 因为在使得 w 和 z 都是有限的那些位处, wdz 没有极. 因此, *每一个微分 wdz 只有有限多个极*.

微分 wdz 在位 $\mathfrak{p}$ 处的留数指的是在展开式 (19.63) 中 π^{-1} 的系数. 在古典理论中, 把微分 wdz 沿着 Riemann 面上围绕点 $\mathfrak{p}$ 的小圆积分再除以 $2\pi i$ 就得到留数. 我们现在一般地证明, 留数不依赖于局部单值化元 π 的选取.

幂级数 (19.63) 可以分成三类项的和：具有 $k<-1$ 的项, 具有 $k=-1$ 的一项和一个没有负指数的幂级数. 最后这个幂级数自然有留数零并且可以把它丢掉. 项 $\alpha_{-1}\pi^{-1}$ 给出留数 α_{-1}, 而且很容易看出, 微分

$$\alpha_{-1}\pi^{-1}d\pi$$

在一个新的局部单值化元 τ 的表达中, 留数同样是 α_{-1}. 因此只需考虑项

$$\pi^{-n}d\pi \quad (n>1), \tag{19.65}$$

并且证明它经过变换

$$\begin{aligned} \pi &= \tau + a_2\tau^2 + \cdots, \\ d\pi &= (1+2a_2\tau+\cdots)d\tau \end{aligned} \tag{19.66}$$

仍然给出留数零.

变换 (19.66) 可以纯形式地在以不定元 $a_2, a_3, \cdots$ 的整系数多项式为系数的 τ 的幂级数所成的整环内进行. 整系数多项式整环可以嵌入有理系数多项式整环内.

有理数的全体构成一个特征为零的域; 当原始的系数域 Δ 有特征 $\mathfrak{p}$ 时, 也可以这样做.

现在证明是容易的. 微分 (19.65) 是函数

$$(-n+1)^{-1}\pi^{-n+1}$$

的微分.

如果将这个函数按 τ 展开, 就得到一个有理系数幂级数

$$\rho_{-n+1}\tau^{-n+1}+\cdots+\rho_{-1}\tau^{-1}+\rho_0+\rho_1\tau+\cdots.$$

这个幂级数的微分是一个不出现 τ^{-1} 项的幂级数与 $d\tau$ 的乘积. 因此经过变换后的留数是零, 这就是所要证的.

当 w 不是域 K 中的函数而是 π 的某一个只含有限个负指数项的幂级数时, 所有这些讨论仍然成立.

现在设 V 是在 19.4 节的意义下的一个向量, 亦即对每一个位 $\mathfrak{p}$, 指定一个幂级数 $V_{\mathfrak{p}}$. 于是我们可以把乘积

$$Vwdz$$

在每一位 $\mathfrak{p}$ 处展成一个幂级数乘以 $d\pi$, 并且确定留数. 设向量 V 的 $\mathfrak{p}$ 分量为

$$V_{\mathfrak{p}}=\sum v_{\mathfrak{p}j}\pi^j, \tag{19.67}$$

并且假设微分 wdz 的展开式为

$$w\frac{dz}{d\pi}d\pi=\left(\sum \alpha_{\mathfrak{p}k}\pi^k\right)d\pi, \tag{19.68}$$

那么留数为

$$r_{\mathfrak{p}}=\sum_{j+k=-1} v_{\mathfrak{p}j}\alpha_{\mathfrak{p}k}. \tag{19.69}$$

因为向量 V 及 wdz 都只有有限多个极, 所以总共只有有限多个不等于零的留数 $\gamma_{\mathfrak{p}}$. 我们可以作它们的和：

$$\sum r_{\mathfrak{p}}=\sum_{\mathfrak{p}}\sum_{j+k=-1} v_{\mathfrak{p}j}\alpha_{\mathfrak{p}k}.$$

这个和就是向量 V 与协向量

$$\lambda=\{\alpha_{\mathfrak{p}j}\} \tag{19.70}$$

在 19.4 节意义下的数量积. 于是有这样的结果：

每一微分 wdz 确定唯一的协向量 λ, 使得数量积 $V\cdot\lambda$ 就是乘积 $Vwdz$ 的留数的和：

$$V\cdot\lambda=\sum r_{\mathfrak{p}}=\sum_{\mathfrak{p}}\sum_{j+k=-1}v_{\mathfrak{p}j}\alpha_{\mathfrak{p}k}. \tag{19.71}$$

现在我们问, 当向量 V 用域 K 中的函数 v 代替时, 这个数量积是什么. 这时数量积 $V\cdot\lambda$ 等于微分

$$vwdz=udz$$

的留数的和, 这里 u 仍是域 K 中一个函数. 这时以下的留数定理成立：

留数定理　*微分 udz 的留数的和总是零.*

在古典函数论中, 这个定理直接由 Cauchy 积分定理推出. 对于完全的常量域, Hasse① 给出了一个一般的证明. 在 19.9 节将给出 Roquette 对 Hasse 证明的一个简化版本.

从留数定理推出, 由微分 wdz 所定义的协向量 λ 是一个在 Weil 意义下的微分.

特别, dz 定义一个在 Weil 意义下的微分, 我们仍然叫它 dz. 这个微分不是零, 因为我们容易找到一个向量 V, 使得 Vdz 有一个非零留数. 若 dz 在位 $\mathfrak{p}$ 处的阶为 m, 只要如此选取向量 V, 使得它的支量 $V_{\mathfrak{p}}$ 等于 π^{-m-1} 而其余一切支量都是零即可.

由于 dz 所定义的微分不等于零, 所以根据 19.6 节, 一切微分 ω 都可以由微分 dz 乘上一个函数 u 而得到. 换句话说：

在 Weil 意义下的一切微分就是古典微分 udz

19.9　留数定理的证明

我要感谢 Roquette 在他的私人通信中提供了以下证明. 这个证明可用于基域是完全域的情形, 而在这里我们假设基域是代数闭的.

我们适当选取 z 使得 K 在 $\Delta(z)$ 上可分. 记 $L=\Delta(z)$, 则 K 是 L 的有限可分扩域, 设为 $K=L(\vartheta)$.

把等式 (18.17) 两边的 t^{n-1} 以及 t^0 的系数分别写成等式, 我们得到

$$N(\vartheta)=\prod N(\vartheta_\nu), \tag{19.72}$$

$$S(\vartheta)=\sum S(\vartheta_\nu). \tag{19.73}$$

① Hasse H. Theorie der Differentiale in algebraischen Funktionenkörpern. J. *reine u. angew. Math.*, 1934, 172: 55.

同样的公式不仅适用于生成元 ϑ, 而且也适用于域 K 的任意元素 u. 为了证明这一点, 我们先作出 u 在域 $L(u)$ 里的范数和迹, 分别记为 $n(u)$ 和 $s(u)$, 这样刚才关于 ϑ 得到的结果也适用于 u:

$$n(u) = \prod n(u_\nu), \tag{19.74}$$

$$s(u) = \sum s(u_\nu). \tag{19.75}$$

设 K 关于 $L(u)$ 的次数是 g, 应用公式 (6.21) 与 (6.22) 可得

$$N(u) = n(u)^g, \tag{19.76}$$

$$S(u) = g \cdot s(u). \tag{19.77}$$

这样就能得到更一般的公式

$$N(u) = \prod N(u_\nu), \tag{19.78}$$

$$S(u) = \sum S(u_\nu). \tag{19.79}$$

现在让我们复习 ϑ_ν 和 u_ν 的定义. 根据 18.5 节, 作为从 L 的已给赋值 φ 开拓到 K 上的赋值 $\varPhi_\nu$, 都是由嵌入 $\vartheta \to \vartheta_\nu$ 确定的. 每个这样的嵌入把域 $K = L(\vartheta)$ 同构地映到完备域 $\varOmega_\nu = \varOmega(\vartheta_\nu)$ 内. 这个域 $\varOmega_\nu$ 是 K 关于赋值 $\varPhi_\nu$ 的完备扩域.

以下我们用位代替赋值. 把域 K 的位记为 $\mathfrak{p}$, 域 L 的位记为 $\mathfrak{q}$. 如果 K 的一个属于位 $\mathfrak{p}$ 的赋值是 L 的一个属于位 $\mathfrak{q}$ 的赋值的开拓, 则称 $\mathfrak{p}$ 是 $\mathfrak{q}$ 的因子, 并记为 $\mathfrak{p}/\mathfrak{q}$. 每个 $\mathfrak{q}$ 只有有限多个因子 $\mathfrak{p}_\nu$, 它们对应于 (18.17) 式里的因子 $F_\nu(t)$. 每个 $\mathfrak{p}_\nu$ 对应一个完备域 $\varOmega_\nu$, 它由单值化元 Π 的幂级数构成. 如果把每个函数 u 映到它的幂级数 u_ν, 就能得到前面所述的同构 $\vartheta \to \vartheta_\nu$, $u \to u_\nu$.

在 $\varOmega_\nu$ 内关于 $\varOmega$ 的范数 $N(u_\nu)$ 也被称为 u 关于位 $\mathfrak{p}$ 的*局部范数*, 记为 $N_\nu(u)$. 关于迹也有类似的结果. 于是, 现在可把公式 (19.78) 和 (19.79) 改写成

$$N(u) = \prod_{\mathfrak{p}/\mathfrak{q}} N_{\mathfrak{p}}(u), \tag{19.80}$$

$$S(u) = \sum_{\mathfrak{p}/\mathfrak{q}} S_{\mathfrak{p}}(u). \tag{19.81}$$

对于每个位 $\mathfrak{p}$ 取一个分量 $V_{\mathfrak{p}}$ 可以定义 K 上向量 V. 利用下面公式可以定义向量 V 的迹为 L 上向量 SV:

$$(SV)_{\mathfrak{q}} = \sum_{\mathfrak{p}/\mathfrak{q}} S_{\mathfrak{p}}(V_{\mathfrak{p}}). \tag{19.82}$$

右边的迹仍然是在完备域 $\Omega_{\mathfrak{p}} = \Omega_\nu$ 内取的. 特别地, 如果 V 是对应于函数 u 的向量, 则根据 (19.81), SV 等于 $S(u)$.

迹映射 $V \to SV$ 是从 K 上所有向量的模 $\mathfrak{Y}(K)$ 到 L 上向量的模 $\mathfrak{Y}(L)$ 的线性映射. 因此, 存在从 L 上协向量模 $\mathfrak{Y}^*(L)$ 到 K 上协向量模 $\mathfrak{Y}^*(K)$ 的对偶映射 S^*, S^* 的定义是

$$V \cdot S^*\rho = SV \cdot \rho, \quad \text{对所有的 } V. \tag{19.83}$$

特别, 当 ρ 是 Weil 微分, 也就是对所有的 $v \in L$ 有 $v \cdot \rho = 0$, 则 $S^*\rho$ 也是 Weil 微分:

$$u \cdot S^*\rho = Su \cdot \rho = 0, \quad \text{对所有的 } u.$$

我们先对有理函数域 $L = \Delta(z)$ 的情形证明留数定理. 设 vdz 是 L 里的经典微分. 有理函数

$$v = \frac{f(z)}{g(z)}$$

可以分裂成多项式加一个分子次数小于分母次数的余式:

$$\frac{f(z)}{g(z)} = q(z) + \frac{r(z)}{g(z)}.$$

微分 $q(z)dz$ 没有留数. 极 ∞ 的单值化元是 $y = z^{-1}$, 有

$$q(z)dz = \left(\sum c_k z^k\right) dz = \sum (-c_k) y^{-k-2} dy,$$

其中不出现含 y^{-1} 的项.

根据 5.10 节, 余式可以分解成部分分式之和

$$\frac{r(z)}{g(z)} = \sum_a \{c_1(z-a)^{-1} + \cdots + c_s(z-a)^{-s}\}.$$

只要对一个部分分式 $c(z-a)^{-k}$ 证明留数定理就够了. 当 $k > 1$ 时, 没有留数. 因此只要考虑以下微分:

$$c(z-a)^{-1}.$$

这个微分在位 a 的留数是 c, 而在位 ∞ 的留数是 $-c$. 所以留数之和等于 0.

现在要把留数定理的一般情形归化到 $L = \Delta(z)$ 的情形, 后者已经利用对偶迹映射获证.

我们把微分 udz 在位 $\mathfrak{p}$ 的留数记为 $\operatorname{res}_{\mathfrak{p}}(udz)$. 若 V 是向量, 乘积 Vdz 在位 $\mathfrak{p}$ 的留数记为 $\operatorname{res}_{\mathfrak{p}}(Vdz)$.

根据公式 (19.71), 微分 dz 定义了一个协向量, 记为 λ_{dz}. 因此, 对任意向量 V 有

$$V\cdot\lambda_{dz}=\sum_{\mathfrak{p}}\operatorname{res}_{\mathfrak{p}}V\,dz. \tag{19.84}$$

设 λ 和 μ 是两个协向量, 如果对于所有的 V, 除了有限个位 $\mathfrak{p}'$ 以外, 每个位 $\mathfrak{p}$ 在 (19.31) 定义的乘积 $V\cdot\lambda$ 和 $V\cdot\mu$ 中都有相等的贡献, 就称它们是几乎相等的.

定理 1 *存在与 λ_{dz} 几乎相等的 Weil 微分 μ_{dz}, 而且这个 μ_{dz} 由这个性质唯一确定.*

证明 微分 dz 也在有理函数域 $L=\Delta(z)$ 里定义了协向量 λ_0. 由于留数定理在 L 里成立, 因此 λ_0 是一个 Weil 微分. 从而对偶迹 $S^*(\lambda_0)$ 也是 Weil 微分, 记为 μ_{dz}:

$$\mu_{dz}=S^*(\lambda_0).$$

对于 K 的每个位 $\mathfrak{p}$, 相伴有 L 的位 $\mathfrak{q}$. 如果位 $\mathfrak{q}$ 处的单值化元 $z-a$ (或 z^{-1}) 也是 $\mathfrak{p}$ 的单值化元, 则称位 $\mathfrak{p}$ 在 L 上是非分歧的. 这时可令 $\Pi=z-a$ 或 $\Pi=z^{-1}$. 此时属于位 $\mathfrak{p}$ 的完备域 $\Omega_{\mathfrak{p}}$ 等于 $z-a$ 的幂级数域 Ω, 并且一个幂级数在位 $\mathfrak{p}$ 的留数等于它在位 $\mathfrak{q}$ 的留数.

除了有限个位以外, 几乎所有的位都在 L 上非分歧. 事实上, 若 $K=L(\vartheta)$ 且 $F(z,t)$ 是以 ϑ 为零点的 t 的不可约多项式, 则 $F(z,t)$ 可被看成 z 与 t 的多项式. F 的判别式是 z 的多项式, 只有有限多个零点. 对于其他的值 $z=a$, $F(a,t)$ 分解成不同素因子的乘积:

$$F(a,t)=c(t-b_1)\cdots(t-b_n).$$

根据 Hensel 引理 (18.4 节), $F(z,t)$ 在 $z-a$ 幂级数的完备域里完全分解成线性因子. 因此, 在分解 (18.17) 中所有的因子 $F_\nu(t)$ 都是线性的, 而且所有的域 $\Omega_\nu=\Omega(\vartheta_\nu)$ 都等于 Ω. 因此 $z-a$ 是所有属于这些域的位的单值化元. 这些域都是非分歧的.

若位 $\mathfrak{p}$ 非分歧, 那么位 $\mathfrak{p}$ 对协向量 μ_{dz} 与 λ_{dz} 作出相等的贡献. 事实上, 若 V 是仅在位 $\mathfrak{p}$ 上异于零的向量, 那么可以假设 V 是 $z-a$ 或 z^{-1} 的幂级数. 此时 V 的局部迹等于 V 自己, 于是

$$\begin{aligned}V\cdot\mu_{dz}&=V\cdot S^*\lambda_0=SV\cdot\lambda_0=V\cdot\lambda_0\\&=\operatorname{res}_{\mathfrak{q}}V\,dz=\operatorname{res}_{\mathfrak{p}}V\,dz=V\cdot\lambda_{dz}.\end{aligned}$$

由此即知 μ_{dz} 几乎等于 λ_{dz}.

还剩下 μ_{dz} 的唯一性有待证明. 我们将证明更一般的结果: *若两个 Weil 微分 λ 和 μ 几乎相等, 则它们一定相等.*

我们令 $\rho=\lambda-\mu$, 并且证明对任意的向量 V 有 $V\cdot\rho=0$. 据 (19.31), 数量积 $V\cdot\rho$ 是各个位 $\mathfrak{p}$ 的贡献之和. 我们可以只考虑有限集 M 里的位 $\mathfrak{p}$ 所作的贡献, 这是因为其他的 $\mathfrak{p}$ 对协向量 ρ 的贡献等于 0. 对于集合 M 里的 $\mathfrak{p}$, 我们可以用 K 的一个函数 u 来近似 V, 使得这些 $\mathfrak{p}$ 对 $(u-V)\cdot\rho$ 的贡献等于 0 (见 19.1 节, 定理 1). 可得

$$(u-V)\cdot\rho=0,$$

由于 ρ 是 Weil 微分, 从而 $V\cdot\rho=u\cdot\rho=0$. 这样就完成了定理 1 的证明.

现在设 y 是另一个元, 使得 K 在 $\Delta(y)$ 上可分. 我们要证明

$$\mu_{dz}=\frac{dz}{dy}\mu_{dy}. \tag{19.85}$$

由于两边都是 Weil 微分, 只要证明两边几乎相等就够了. 现在 μ_{dy} 几乎相等于 λ_{dy}, μ_{dz} 几乎相等于 λ_{dz}. 所以只要证明

$$\lambda_{dz}=\frac{dz}{dy}\lambda_{dy} \tag{19.86}$$

就可以了. 而由定义 (19.84) 立即可得

$$\begin{aligned}V\cdot\lambda_{dz}&=\sum_{\mathfrak{p}}\mathrm{res}_{\mathfrak{p}}\,V\,dz=\sum_{\mathfrak{p}}\mathrm{res}_{\mathfrak{p}}\,V\frac{dz}{dy}dy\\&=V\frac{dz}{dy}\cdot\lambda_{dy}=V\cdot\frac{dz}{dy}\lambda_{dy}.\end{aligned}$$

最后我们要证明

$$\lambda_{dz}=\mu_{dz}. \tag{19.87}$$

设 $\mathfrak{p}$ 是一个位, y 是单值化元. 在 19.8 节证明了 z 在 $\Delta(y)$ 上可分. 由于 K 在 $\Delta(z)$ 上可分, $\Delta(z)$ 在 $\Delta(y)$ 上可分, 因此 K 在 $\Delta(y)$ 上可分. 此外 $\mathfrak{p}$ 在 $\Delta(y)$ 上非分歧, 因此 λ_{dy} 和 μ_{dy} 的 $\mathfrak{p}$ 分量相等:

$$(\lambda_{dy})_{\mathfrak{p}}=(\mu_{dy})_{\mathfrak{p}}.$$

由此可得

$$(\lambda_{dz})_{\mathfrak{p}}=\left(\frac{dz}{dy}\lambda_{dy}\right)_{\mathfrak{p}}=\left(\frac{dz}{dy}\mu_{dy}\right)_{\mathfrak{p}}=(\mu_{dz})_{\mathfrak{p}}.$$

这对任意的 $\mathfrak{p}$ 都成立, 从而断言 (19.87) 也正确.

所以我们不再需要区分 λ_{dz} 与 μ_{dz}. 由于 μ_{dz} 是 Weil 微分, 因此 λ_{dz} 也是 Weil 微分, 也就是说留数定理是正确的.

第20章　拓 扑 代 数

拓扑代数所研究的是那样的群、环和体, 它们同时是拓扑空间, 而且代数运算在拓扑意义下是连续的. 我们称它们为拓扑群、拓扑环和拓扑体, 或简称 T 群、T 环和 T 体.

20.1　拓扑空间的概念

一个拓扑空间是一个集合 T, 其中某些子集被指定作为开集. 它们具有下列性质:

I. 有限多个开集的交仍是开集

II. 任意多个开集的并仍是开集.

例　设 T 是一个有序集. T 中的开区间由 $a < x < b$ 或 $a < x$ 或 $x < b$ 所定义. 一个开集就是这样的集合, 它在包含元素 y 的同时, 也一定包含一个含 y 的开区间.

例　设 T 是复数域. 绕 a 的圆盘由 $|z-a| < \varepsilon$ 所定义. T 中的开集就是这样的集合, 它在包含元素 a 的同时, 也一定包含一个绕 a 的圆盘.

例　同样的定义对每一个赋值域都适用. 只要用 $\varphi(z-a)$ 代替 $|z-a|$ 即可. 所以每一个赋值域都是一个拓扑空间.

特别, 从 I 得出, 整个空间 T 是开的, 因为它可以看作开集的交, 这些开集所成的集是空集. 同样从 II 得出, 空集是开集, 因为空集也可以看作开集的并, 这些开集所成的集是空集.

一个子集 M 叫做在 T 中是闭的, 如果它在 T 中的余集是开集. 对于闭集有与 I 和 II 等价的法则:

I$'$. 有限多个闭集的并仍是闭集.

II$'$. 任意多个闭集的交仍是闭集.

集合 T 中的元素叫做空间 T 的点. 含点 p 的开集叫做 p 的开邻域. 任意一个包含着 p 的一个开邻域的集合叫做 p 的一个邻域, 并且记作 $U(p)$.

对于拓扑空间 T 的一个子集 T', 如果以 T' 与 T 的开集的交作为 T' 的开集, 则 T' 仍是一个拓扑空间. 性质 I 和 II 显然被满足.

T 的一个子集 M 的闭包 $\overline{M}$ 指的是一切含 M 的闭集的交.

习题 20.1　一个点 p 属于闭包 $\overline{M}$ 当且仅当 p 的每一邻域中都有 M 的点.

习题 20.2　Kuratowski 定义一个拓扑空间为一个集合 T, 在其中对于每一子集 M 有一个子集 $\overline{M}$ 与它对应, $\overline{M}$ 称为 M 的闭包, 并且具有下列性质：

(a) $M \cup N$ 的闭包是 $\overline{M} \cup \overline{N}$,

(b) $\overline{M}$ 包含 M,

(c) $\overline{M}$ 的闭包就是 $\overline{M}$,

(d) 空集的闭包是空集.

再定义, 若 $\overline{M} = M$, 则称 M 是闭集; 若 M 在 T 中的余集是闭集, 则称 M 是开集. 证明：Kuratowski 的定义与这里所给的拓扑空间的定义是等价的.

提示：首先从 (a) 得出, 当 $M \subseteq N$ 时 $\overline{M} \subseteq \overline{N}$. 然后从 (a)～(c)：$\overline{M}$ 是所有含 M 的闭集 $\overline{N} = N$ 的交. 于是就得出法则 I′ 和 II′. 反之, 从 I′ 和 II′ 可推出 (a)～(d).

如果集合 M 的闭包等于 T, 或者 T 的每个点的任意邻域包含 M 的点, 则称 M在 T 内稠密.

20.2　邻　域　基

点 p 的一组邻域 $U(p)$ 说是构成 p 的一个邻域基, 如果 p 的每一个邻域都至少包含这组邻域中的一个邻域 $U(p)$. 要做到这一点, 只要 p 的每一开邻域都包含这个邻域组的一个邻域 $U(p)$ 就可以了. 例如, 点 p 的所有开邻域构成 p 的一个邻域基. 在例 1 中, 所有含 p 的开区间构成 p 的一个邻域基. 在例 2 中, 所有绕 a 的圆盘构成 p 的一个邻域基.

常常用这样的方法来决定拓扑空间. 首先给出每一点的一个邻域基, 然后像在我们的例子里所做的那样, 利用这些基来定义开集. 首先对每一点 p 令某一组基集 $U(p)$与它对应, 并且下列条件被满足：

(U_1) *对每一点 p 都有一组基集 $U(p)$ 并且其中每一个都含有 p.*

(U_2) *对于两个基集 $U(p)$ 和 $V(p)$ 存在一个基集 $W(p)$, 它含于 $U(p)$ 和 $V(p)$ 的每一个里面.*

我们现在用基集来定义开集 M为这样的集合, 若 M 含有点 p, 则 M 必含有一个整个的基集 $U(p)$. 这样定义的开集显然具有性质 I 和 II. 从而给出一个拓扑空间, 为了使得基集 $U(p)$ 在这一拓扑的意义下也是邻域, 它们还必须满足另外的条件. 一个充分的条件就是要求 $U(p)$ 也是开集：

(U_3) *若 q 属于 $U(p)$, 则 $U(p)$ 含有一个基集 $V(q)$.*

下面的较弱的条件是充分且必要的：

(U_3') *每一个基集 $U(p)$ 总含有一个基集 $V(p)$, 使得对 $V(p)$ 中每一点 q 都有一个基集 $W(q)$ 含于 $U(p)$ 中.*

若 (U_3') 成立, 那么在 $U(p)$ 中就可以定义一个集合 U', 它由所有那样的点 q

所组成, 对于 q 有基集 $W(q)$ 含于 $U(p)$ 中. 这个集合显然是开的并且含有 p. 因此 $U(p)$ 含有 p 的一个开邻域, 即 $U(p)$ 是 p 的一个邻域.

现在我们不再用基集这个词. 以后我们总把基集叫做*基邻域*. 所有点 p 的基邻域的全体叫做拓扑空间 T 的一个*邻域基*或*邻域组*.

邻域组这个概念首创于 Hausdorff. 这一概念只用到开邻域. $(\mathrm{U}_1) \sim (\mathrm{U}_3)$ 这三个要求正是前三个邻域公理. 第四个是 Hausdorff 的分离公理, 我们将在 20.4 节中提出.

例 在实数域上 n 维向量空间中, 可以定义围绕向量 $(b_1, \cdots, b_n)$ 的边长为 2ε 的*方体*是满足条件

$$|a_i - b_i| < \varepsilon \quad (i = 1, \cdots, n)$$

的向量 $(a_1, \cdots, a_n)$ 的全体.

方体满足条件 $(\mathrm{U}_1) \sim (\mathrm{U}_3)$. 于是这个向量空间是以方体为邻域基的拓扑空间.

如果一个拓扑空间的所有子集都是开集, 就被称为*离散的*. 此时单独的点构成邻域基.

习题 20.3 两个集合组 $U(p)$ 与 $V(p)$ 定义同一个拓扑空间, 必要且只要每一个集合 $U(p)$ 含有一个 $V(p)$ 而且每一个 $V(p)$ 含有一个 $U(p)$.

习题 20.4 通过方体所定义的向量空间的拓扑与向量空间的基的选择无关.

20.3 连 续, 极 限

拓扑空间 T 映入拓扑空间 T' 的一个函数 $p' = f(p)$ 说是*在点* p_0 *处连续*, 如果对于 $f(p_0)$ 在 T' 内的每一邻域 U', 都有 p_0 在 T 内的一个邻域 U, 使得 U 的象完全包含在 U' 内.

同样地, 变量 p 和 q 分别在 T_1 和 T_2 中而值在 T_3 中的一个函数 $f(p, q)$ 说是在点 (p_0, q_0) 处连续, 如果对于 $f(p_0, q_0)$ 的每一邻域 W 都有 p_0 的一个邻域 U 和 q_0 的一个邻域 V, 使得当 p 在 U 内而 q 在 V 内时, 总有 $f(p, q)$ 在 W 内.

如果一个函数在每一点处都连续, 就叫做一个*连续函数*或*连续映射*. 一个映射 $p' = f(p)$ 是连续的, 当且仅当 T' 中任一开集 U' 的原象 (即 T 中这样的元素所成的集合, 它们的象属于 U') 总是开集.

T 到 T' 上的一对一的双方连续的映射叫做*拓扑映射*. 拓扑映射将开集映成开集, 将闭集映成闭集.

拓扑空间 T 中的一个点列 $\{p_\nu\}$ 说是*收敛于极限* p, 如果点 p 的每一邻域 $U(p)$ 总包含这个序列中从某一指标以后的所有点:

$$p_\nu \in U(p) \quad 对 \nu \geqslant k.$$

在这里, 我们总可以把邻域 $U(p)$ 限于 p 的某邻域基中的邻域, 因为每一邻域都含有这样一个基邻域.

习题 20.5　连续映射保持极限关系.

习题 20.6　连续函数的连续函数仍是连续的.

20.4　分离公理和可数公理

最重要的拓扑空间除了满足公理 I 和 II 以外还满足下列的第一分离公理:

(T_1) *若 $p \neq q$, 则存在 p 的一个邻域, 它不含 q.*

具有性质 (T_1) 的空间叫做 T_1空间. 下列表述形式是与它等价的:

单独一个点的闭包就是这一点本身.

比 (T_1) 较强的是第二分离公理, 或称 Hausdorff 分离公理:

(T_2) *若 $p \neq q$, 则存在互不相交的邻域 $U(p)$ 与 $U(q)$.*

若空间满足 (T_2) 就称为 T_2空间或Hausdorff 空间.

第一可数公理是:

(A_1) *每一点 p 都有一组可数的邻域基.*

较强的第二可数公理我们将用不到.

对于我们来说, 重要的拓扑空间是既满足第一分离公理又满足第一可数公理的空间. 对于拓扑群, 因而也对于拓扑环和拓扑体 (它们都是加法群), 我们将证明, 第二分离公理乃是第一分离公理的推论.

在这里所引入的一些拓扑概念只是选择了一些最必需的基本概念. 如果想知道更多的拓扑知识, 可以首先学习Alexandroff 和 Hopf 的书: *Topologie* I (Springer, Grundlehren, Band XLV, 1935), 然后再阅读一些新的文献.

习题 20.7　在一个 Hausdorff 空间中, 点列 $\{p_\nu\}$ 最多只能有一个极限.

习题 20.8　若拓扑空间满足 (A_1), 那么一个集合 M 的闭包是由 M 中一切收敛点列的极限所组成. 如果所有这些极限都在 M 中, 则 M 是闭集.

20.5　拓　扑　群

一个拓扑群(或简称 T 群) 是一个拓扑空间, 同时又是一个群, 使得 xy 是 x 和 y 的连续函数且 x^{-1} 是 x 的连续函数. 因此, 除了群的四个公理和开集的两个基本性质外, 还要加上两个要求:

(TG_1) *对于乘积 ab 的每一邻域 $U(ab)$, 存在邻域 $V(a)$ 和 $W(b)$, 使得乘积 $V(a)W(b)$ 含于 $U(ab)$ 中.*

(TG_2) *对于每一邻域 $U(a^{-1})$, 存在邻域 $V(a)$, 使得 $V(a)^{-1}$ 含于 $U(a^{-1})$ 中.*

这里 M^{-1} 理解作 M 中所有元素 x 的逆元 x^{-1} 所成的集.

显然, 对于 (TG_1) 和 (TG_2) 中的邻域 U, 只要求是邻域基里的邻域就可以了, 而且 $V(a)$ 和 $W(b)$ 总可以选为基邻域.

拓扑群的例子是：

(a) 实数加群或复数加群.

(b) n 维实向量空间 (20.2 节, 例 4).

(c) 不等于零的实数或复数所成的乘法群.

每一个群 G 都可以成为*离散拓扑群*, 只要我们取离散拓扑, 即 G 中所有子集都取作开集即可.

进一步的例子可以看习题 20.10 和 20.7 节例 5.

从 (TG_1) 和 (TG_2) 容易得出：

(TG') 对于邻域 $U(a^{-1}b)$, 存在邻域 $V(a)$ 和 $W(b)$, 使得 $V(a)^{-1}W(b)$ 含于 $U(a^{-1}b)$ 中.

(TG'') 对于邻域 $U(ab^{-1})$, 存在邻域 $V'(a)$ 和 $W'(b)$, 使得 $V'(a)W'(b)^{-1}$ 含于 $U(ab^{-1})$ 中.

习题 20.9　证明：性质 (TG') 和 (TG'') 中任何单独一个都可以用来代替性质 (TG_1) 和 (TG_2).

现在我们来证：

凡是 T_1 群都是 T_2 群.

证　设 $a \neq b$, 则 $a^{-1}b \neq e$. 由 (T_1), 存在邻域 $U(a^{-1}b)$, 它不含 e. 由 (TG'), 存在 $V(a)$ 和 $W(b)$, 使得 $V(a)^{-1}W(b)$ 含于 $U(a^{-1}b)$ 中, 从而 $V(a)^{-1}W(b)$ 不含 e. 因此 $V(a)$ 与 $W(b)$ 互不相交. 这就证明了 (T_2).

如果在一个 T 群里有一个 p 的邻域, 它不包含 q, 则存在两个不相交的邻域 $U(p)$ 和 $U(q)$. 因此, 也存在不包含 p 的邻域 $U(q)$. 在这个情形, p 和 q 称为*可分的*. 与 p 不可分的点 q 构成了集合 $\{p\}$ 的闭包.

两个拓扑群 G 与 H 称为*拓扑同构的*, 如果存在 G 到 H 上的一个同构映射, 它同时又是一个拓扑映射.

20.6　单位元的邻域

如果给出了单位元 e 的一个邻域基, 那么就可以知道 e 的所有邻域：这就是至少含一个基邻域的集合 $U(e)$. 这样一来, 其他点的邻域也就知道了. 事实上, 设 $U(e)$ 是 e 的一个邻域, 则 $aU(e)$ 就是 a 的一个邻域, 并且 a 的所有邻域都可以这样得到. 我们称 $aU(e)$ 为一个“从 e 平移到 a”的邻域.

我们看到, 当 e 的一个邻域的基给定时, 一个 T 群的拓扑就完全决定了. 我们用 U(或 V,W) 来表示这样一个基中的邻域.

一组集合 U 必须满足什么条件才能使带着平移邻域 $U(a)=aU$ 的群 G 成为一个拓扑群呢?

无论如何, 下列条件是必要的:

(E_1) 每一 U 都含有 e(从 20.2 节的 (U_1) 得出).

(E_2) 对于每一 U, 存在一个 V, 使得 $V\cdot V$ 含于 U 中.

(E_3) 对于每一 U, 存在一个 V, 使得 V^{-1} 含于 U 中(由 20.5 节的 (TG_2) 得出).

(E_4) 每一个变换所得的集 aUa^{-1} 含有一个 V.

(E_5) 每一个交 $U\cap V$ 含有一个 W(由 20.2 节的 (U_2) 得出).

($\mathbf{E}_2$) 的证明　按 (TG_1), 对于每一 U, 存在 V' 及 W', 使得 $V'W'$ 含于 U 中. 按 (U_2), 在交 $V'\cap W'$ 中含有一个 V.

($\mathbf{E}_4$) 的证明　因为 $a^{-1}xa$ 是 x 的连续函数, 所以对于 U 存在一个 V, 使得 $a^{-1}Va$ 含于 U 中, 即 V 含于 aUa^{-1} 中.

现在反过来, 设在群 G 中有一组集合 U, 它满足条件 (E_1) ~(E_5). 我们做平移集合 aU, 取它们作为点 a 的基邻域. 显然, 这组基邻域具有 20.2 节的性质 (U_1) 和 (U_2). 我们证明, 它也具有性质 (U_3').

设 $U(a)=aU$. 由 (E_2), 存在一个 V 使得 $V\cdot V$ 含于 U 中. 若 x 是 aV 中的一点, 则 xV 在 aVV 中, 从而含于 aU 中. 这就证明了 (U_3')

现在来证 20.5 节的 (TG_1) 和 (TG_2).

设给定一个邻域 abU. 由 (E_2), 存在一个 V, 使得 $V\cdot V$ 含于 U 中. 由 (E_4), 存在一个 W 含于 bVb^{-1} 中. 于是

$$aW\cdot bV\subseteq abVb^{-1}\cdot bV=abV\cdot V\subseteq abV.$$

这就证明了 (TG_1).

设给定一个邻域 $a^{-1}U$. 于是根据 (E_3), 存在一个 V, 使得 V^{-1} 含于 U 中. 又根据 (E_4), 在 $a^{-1}Va$ 中存在一个 W.

于是 $aW\subseteq Va$, 从而

$$(aW)^{-1}\subseteq(Va)^{-1}=a^{-1}V^{-1}\subseteq a^{-1}U.$$

这就证明了 (TG_2).

因此, 要把一个群做成 T 群, 只要给出单位元的一个邻域基, 并且证明性质 (E_1) ~(E_5) 成立即可.

(E_2) 和 (E_3) 可以合并成为一条:

(E_{2+3}). 对于每一 U, 存在一个 V, 使得 $V^{-1}V\subseteq U$.

对于交换群来说, (E_4) 是多余的. 这时把运算写成加法, 那么零元的邻域只要满足三个要求：

(1) *每一 U 都含有零.*

(2) *对于每一 U, 存在一个 V 使得 $V-V\subseteq U$.*

(3) *每一个交 $U\cap V$ 都含有一个 W.*

要使得由单位元的邻域所决定的 T 群是一个 T_1 群, 下列分离公理必须被满足：

(E_6) *对每一 $a\neq e$, 存在一个不含 a 的 U.*

我们可以把 (E_1) 和 (E_6) 合并成为一条：

(E_{1+6}) *一切 U 的交是仅含单位元的集.*

对于加群相应的要求是：

一切 U 的交是仅含零元的集.

如果 G 不是 T_1 群, 那么在 e 的所有邻域里都还含有不同于 e 的其他元素 p, 这些元素与 e 不可分. 它们构成 G 的正规子群 N. 根据 20.5 节, N 是集合 $\{e\}$ 的闭包, 因此 N 是闭集. 商群 G/N 是 T_1 群.

习题 20.10　设在一群 G 中给出了一个正规子群列

$$H_1\supset H_2\supset\cdots.$$

用这些正规子群定义作为单位元的邻域基, 那么性质 (E_1) ∼(E_5) 都被满足, 而 G 成为一个 T 群. (E_6) 仅当所有 H_i 的交只含单位元时才能成立.

20.7　子群和商群

一个 T 群的每一个子群仍是一个 T 群. 闭子群具有特别的重要性. 我们首先证明：

每一个开子群都是闭的.

证　设子群 H 是 G 中的开集. 那么陪集 aH 在 G 中仍然是开的. 除掉 H 后所有陪集的并仍是开集. 这个并是 H 的余集, 所以 H 是闭的.

例　设 R 是有理数域上一切 n 阶方阵所成的环. R 中的可逆元素是具有逆方阵 A^{-1} 的方阵 A. 所有这些可逆元素做成一个群 G. 把满足条件

$$|b_{ik}-a_{ik}|<\varepsilon$$

的方阵 B 的全体定义作为方阵 A 的方体邻域 (参考 20.2 节, 例 4). 于是 R 是一个加法拓扑群而 G 是一个乘法拓扑群. 在 G 中, 行列式 D 为正的一切方阵 A 是 G 的一个子群. 这个子群在 G 中是开的, 因此也是闭的.

现在设 H 是 G 的一个正规子群, 暂时先不要求它是闭的. 我们作商群

$$G/H = \overline{G}.$$

通过 G 到 $\overline{G}$ 上的同态映射 $a \to \overline{a}$ 把 e 的基邻域 U 映成 $\overline{G}$ 的子集 $\overline{U}$, 这些 $\overline{U}$ 显然仍满足 $(E_1) \sim (E_5)$ 的要求. 用这些集合 $\overline{U}$ 在 $\overline{G}$ 中定义一个拓扑. 映射 $a \to \overline{a}$ 在这个拓扑意义下是连续的, 这一点可以直接从连续性的定义推出. 于是有

T 群的每一个商群 G/H 是一个 T 群, 并且映射 $a \to \overline{a}$ 是连续的.

我们现在问, 在什么条件下, 商群 G/H 满足第一分离公理 (T_1). 答案是:

当正规子群 H 在 G 中是闭的时候, G/H 是一个 T_1 群. 反过来也对.

证　设 H 在 G 中是闭的. 那么每一陪集 aH 在 G 中都是闭的. 若 $\overline{a} \neq \overline{e}$, 则 e 不在 aH 内, 即 e 属于 aH 的开余集. 因此存在 e 的一个邻域 U, 它与 aH 不相交. 于是 U 在 $\overline{G}$ 中的象 $\overline{U}$ 不含有 $\overline{a}$. 所以 $\overline{G}$ 满足 (E_6). 从而 $\overline{G}$ 是一个 T_1 群.

现在设 $\overline{G}$ 是一个 T_1 群. 那么 $\overline{G}$ 中不等于 $\overline{e}$ 的元素 $\overline{a}$ 所成的集合在 $\overline{G}$ 中是开的. 因为映射 $a \to \overline{a}$ 是连续的, 所以这个开集的原象也是开的. 然而这个原象恰是 H 的余集. 所以 H 在 G 中是闭的.

习题 20.11　设 H 是 G 的一个子群, N 是 G 的一个正规子群. 若 N 在 G 中是闭的, 则交 $D = N \cap H$ 在 H 中是闭的, 并且 H/D 到 NH/N 上的自然映射是连续的.

20.8　T 环和 T 体

一个拓扑环(简称 T 环) 是一个拓扑空间, 它同时又是一个环, 并且要求 $x+y, -x$ 和 xy 都是连续函数. 代替上述要求, 我们也可以要求 $x-y$ 和 xy 是 x 和 y 的连续函数, 即

(TR_1) *对于每一邻域 $U(a-b)$, 存在 $V(a)$ 和 $W(b)$, 使得所有 $V(a)$ 的元素与 $W(b)$ 的元素之差都属于 $U(a-b)$.*

(TR_2) *对于每一邻域 $U(ab)$, 存在 $V(a)$ 和 $W(b)$, 使得所有 $V(a)$ 的元素与 $W(b)$ 的元素之积都属于 $U(ab)$.*

对于一个 T 体, 除了上面的要求以外, 还要求 x^{-1} 是 x 的连续函数, 即

(TS) *对于每一邻域 $U(a^{-1})$, 存在 $V(a)$, 使得 $V(a)$ 中每一个元素的逆元都属于 $U(a^{-1})$.*

如果 (TS) 被满足, 那么上面的环拓扑也叫做一个*体拓扑*.

交换的 T 体自然地叫做 T *域*.

一个环对于加法来说是一个交换群. 为了在这个群里定义拓扑, 只要按 20.5 节, 定义零元素的基邻域 $U, V, \cdots$ 使 20.6 节中的要求 (1)~(3) 被满足就可以了. 要使得乘法也是连续的, 还必须满足下列要求:

(4) 对于 a, b 和 U, 存在 V 和 W, 使得

$$(a+V)(b+W) \subseteq ab+U.$$

一个拓扑体除此之外, 还必须满足下列与 (TS) 等价的条件：

对于 $a \neq 0$ 和 U, 存在一个 V, 使得

$$(a+V)^{-1} \subseteq a^{-1}+U. \tag{20.1}$$

我们可以令 $aU = U', Va^{-1} = V'$, 即 $U = a^{-1}U', V = V'a$. 于是由 (20.1) 得

$$a^{-1}(1+V')^{-1} \subseteq a^{-1}(1+U')$$

或

$$(1+V')^{-1} \subseteq 1+U'. \tag{20.2}$$

因此, 只要 (20.1) 对于 $a = 1$ 成立就够了. 所以公理 (TS) 等价于下列条件：

(5) 对于零元素的每一邻域 U, 存在零元素的一个邻域 V, 使得

$$(1+V)^{-1} \subseteq 1+U. \tag{20.3}$$

一切赋值域都是 T 域的例子, 特别地, 实数域、复数域和 p 进数域以及它们的子域都是 T 域.

一切实 n 阶方阵是一个 T 环. 在这里, 零方阵的一个基邻域 U 是由这样的方阵所成的集合, 其中每一方阵的元素的绝对值都小于 ε.

更进一步还有这样的例子. 设在环 $\mathfrak{o}$ 中有一连串的双边理想列

$$\mathfrak{g}_1 \supseteq \mathfrak{g}_2 \supseteq \cdots.$$

把这些理想取作零元素的基邻域. 那么 (1)~(4) 的要求被满足. 如果所有 $\mathfrak{g}_\nu$ 的交只含有零元素, 那么就得到一个 T_1 环.

由序列 $\{\mathfrak{g}_\nu\}$ 所定义的环拓扑称为$\{\mathfrak{g}_\nu\}$-adic 拓扑. 特别, 当 $\mathfrak{g}_\nu$ 是交换环 $\mathfrak{o}$ 中某一个素理想 $\mathfrak{p}$ 的幂时,

$$\mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \cdots,$$

那么这样定义的拓扑叫做一个 $\mathfrak{p}$-adic 拓扑. 以后将会看到, 在许多重要的情形下, $\mathfrak{p}$ 的所有幂的交是零理想, 这时分离公理 (T_1) 被满足.

在 18.1 节里曾利用素理想 $\mathfrak{p}$ 的幂 $\mathfrak{p}^\nu$ 的序列在较强的条件下作出环 $\mathfrak{o}$ 的赋值. 然而, 当我们只要求一个环拓扑而不要求赋值的时候, 这些限制条件是不必要的.

习题 20.12 要求 (4) 可以用下列三个要求来代替：

(a) 对于 a 和 U, 存在 V, 使得 $aV \subseteq U$;

(b) 对于 b 和 U, 存在 V, 使得 $Vb \subseteq U$;

(c) 对于 U 存在 V, 使得 $VV \subseteq U$.

习题 20.13　在实数域上的四元数体 (参考 13.2 节, 例 2) 内, 我们可以这样定义零的邻域: U_ε 由所有这样的四元数 $a+bj+ck+dl$, 它的模

$$(a-bj-ck-dl)(a+bj+ck+dl)=a^2+b^2+c^2+d^2$$

小于 ε, 所组成. 证明: 具有这个拓扑的四元数体是一个 T_1 体.

20.9　用基本序列作群的完备化

在 18.2 节中曾经对每一赋值域作一个扩域, 使得在扩域中 Cauchy 收敛定理成立. 在那里, 基本序列 $\{a_\nu\}$ 是一个重要的工具. 它是这样定义的: 对于充分大的 μ 与 ν, $a_\nu - a_\mu$ 将属于零元素的任一事先指定的邻域. 在这里, 我们将按照 van Dantzig① 的做法对于 T 群给出一个类似的构造.

设有 T 群中一个元素列 $\{x_\nu\}$. 如果对于单位元素的任一邻域, 存在 $m>0$, 使当 $\mu \geqslant m$ 及 $\nu \geqslant m$ 时, 商 $x_\mu^{-1}x_\nu$ 恒在所给的邻域内, 那么就说 $\{x_\nu\}$ 为一个基本序列或Cauchy 序列.

如果每一个基本序列在群本身中有一极限, 就说这个 T 群是*弱完备的*.

我们的目的是要证明, 每一个满足公理 (T_1) 和 (A_1) 的 T 群可以扩张为一个弱完备群.

下面一个引理的证明, 我们要感谢 Fischer.

引理　*设 $\{x_\nu\}$ 是一个基本序列. 那么对于每一 U 都存在一个 V 和一个 m, 使得*

$$x_\mu^{-1}Vx_\mu \subseteq U, \quad 对\ \mu \geqslant m. \tag{20.4}$$

证　取 W 使得 $WWW \subseteq U$. 再取 m, 使

$$x_\mu^{-1}x_\nu \in W, \quad 对\ \mu \geqslant m, \nu \geqslant m.$$

那么特别对于 $\mu \geqslant m, x_\mu^{-1}x_m$ 及 $x_m^{-1}x_\mu$ 总在 W 内. 根据 (E_4), 可以在 $x_mW_m^{-1}$ 中取 V. 于是

$$x_\mu^{-1}Vx_\mu \subseteq x_\mu^{-1}x_mWx_m^{-1}x_\mu \subseteq WWW \subseteq U, \quad 对\ \mu \geqslant m.$$

从这个引理得

① van Dantzig D. Zur Topologischen Algebra I: Komplettierungstheorie. *Math. Ann.*, 1933, 107: 587.

推论 I 若 $\{x_\mu\}$ 和 $\{y_\mu\}$ 是两个基本序列, 则 $\{x_\mu y_\mu\}$ 也是一个基本序列.

证 我们有

$$(x_\mu y_\mu)^{-1}x_\nu y_\nu = y_\mu^{-1}(x_\mu^{-1}x_\nu)y_\mu \cdot y_\mu^{-1}y_\nu.$$

在等号右端的乘积里, 可以使两个因子都在 e 的任意小的邻域内: 第一个因子是由于上述引理, 而第二个因子则是由于基本序列的定义. 这样一来, 乘积也在 e 的一个任意邻域内. 我们称 $\{x_\mu y_\mu\}$ 是基本序列 $\{x_\mu\}$ 与 $\{y_\mu\}$ 的乘积.

引理的另一推论是:

推论 II 若 $\{x_\mu\}$ 是一个基本序列, 且 $\{y_\mu\}$ 收敛于 e, 则

$$\{x_\mu^{-1}y_\mu x_\mu\}$$

也收敛于单位元 e.

证 由引理, 对于充分大的 μ, 有 $x_\mu^{-1}Vx_\mu \subseteq U$; 又对于充分大的 μ, y_μ 属于 V. 因此对于充分大的 μ, $x_\mu^{-1}y_\mu x_\mu$ 属于 U.

要使得 G 可以扩充为一个完备拓扑群, 下列完备公理是必需的:

(TG_3). 若 $\{x_\mu\}$ 是一个基本序列, 则 $\{x_\mu^{-1}\}$ 也是一个基本序列.

在一个交换群里, (TG_3) 是自动满足的, 因为当 $x_\mu^{-1}x_\nu$ 在 U 内时,

$$x_\nu x_\mu^{-1} = (x_\nu^{-1})^{-1}x_\mu^{-1}$$

也在 U 内. 但是在一般情形, (TG_3) 不是其余公理的结果.

从推论 I 和 (TG_3) 直接得出, 基本序列作成一个群 F. 群 F 的单位元是基本序列 $\{e\}$.

我们现在把 F 作成一个拓扑群. 为此, 我们这样来定义单位元 $\{e\}$ 的基邻域 $\overline{U}$: $\overline{U}$ 是由这样的基本序列 $\{x_\nu\}$ 所组成, 对充分大的 ν, 所有元素 x_ν 都在 U 内.

这些邻域 $\overline{U}$ 满足要求 (E_1) $\sim$ (E_5)(20.6 节), 对于 (E_1) $\sim$ (E_3) 和 (E_5) 是显然的, 而 (E_4) 就是上面的引理: 若 $\{x_\mu\}$ 是一个基本序列, 则存在 V 使得对于充分大的 μ 有

$$x_\mu^{-1}Vx_\mu \subseteq U \quad \text{或} \quad V \subseteq x_\mu U x_\mu^{-1}.$$

这样一来, F 是一个拓扑群. 在这个群中, 所有收敛于 e 的基本序列作成一个子群 N, 而且由推论 II, 它还是一个正规子群. 我们现在证明, N 在 F 中是闭的.

若一基本序列 $\{x_\mu\}$ 不属于 N, 即不收敛于 e, 那么就存在邻域 U, 它不包含这个基本序列的几乎所有的元素. 按照 (E_2) 和 (E_3), 就存在一个 V, 使得

$$VV^{-1} \subseteq U.$$

这个 V 在 F 中决定一个邻域 $\overline{V}$, 它由几乎所有元素 y_μ 都在 V 内的基本序列 $\{y_\mu\}$ 所组成. 我们说, 在 F 里 $\{x_\mu\}$ 的邻域 $\{x_\mu\}\overline{V}$ 整个地含于 N 在 F 中的余集.

事实上, 如果 $\{x_\mu\}\overline{V}$ 与 N 有一个公共基本序列

$$\{x_\mu\}\{y_\mu\} = \{x_\mu y_\mu\} = \{z_\mu\},$$

这里几乎所有 y_μ 都在 V 内, 而 $\{z_\mu\}$ 收敛于 e. 那么几乎所有 z_μ 都在 V 内. 因此几乎所有

$$x_\mu = z_\mu y_\mu^{-1}$$

都在 VV^{-1} 内, 从而也在 U 内, 这与 U 的定义矛盾. 所以 $\{x_\mu\}\overline{V}$ 与 N 没有公共元素.

这样一来, N 在 F 中的余集是一个开集, 即 N 在 F 中是闭的. 因此按 20.7 节, F/N 是一个 T_1 群.

在 F 中, 常值基本序列 $\{a\}$ 作成一个子群 G', 它与所给的群 G 是拓扑同构的. 由于分离公理 (T_1), 这个子群 G' 与 N 只有 $\{e\}$ 是公共的. 我们可以把常值基本序列 $\{a\}$ 与元素 a 等同起来, 从而把 G' 与 G 等同起来. 我们现在作关于 N 的同余类, 于是 G' 就变到一个商群 G'', 它是 F/N 的一个子群, 从而它仍然是一个 T 群. 这个 T 群与 G' 拓扑同构, 从而也与 G 拓扑同构. 因此我们仍然可以把它与 G 等同起来.

现在令 $F/N = \widetilde{G}$. 这样就将 G 嵌入一个 T_1 群 $\widetilde{G}$. 我们首先证明:

推论 III　如果基本序列 $\{x_\mu\}$ 决定 $\widetilde{G}$ 中的元素 $\widetilde{x}$, 则

$$\lim x_\mu = \widetilde{x}. \tag{20.5}$$

证　设基本序列 $\{x_\mu\}$ 作为 F 中的元素考虑时, 记作 $\overline{x}$. 通过由 F 到 $F/N = \widetilde{G}$ 上的同态映射, $\overline{x}$ 被映成 $\widetilde{x}$. 这个映射是连续的. 因此, 为了证明 (20.5), 只要证明在 F 中相应的关系

$$\lim x_\mu = \overline{x} \text{ 在 } F \text{ 内}. \tag{20.6}$$

关系 (20.6) 表示, 对于充分大的 $\mu, \overline{x}^{-1}x_\mu$ 在 $\overline{U}$ 内, 或者根据 $\overline{U}$ 的定义, 这就表示对于充分大的 μ 和 ν,

$$x_\nu^{-1}x_\mu \text{ 在 } U \text{ 内}.$$

然而这是显然的, 因为 $\{x_\mu\}$ 是一个基本序列.

现在已经达到可以证明主要定理的地步了.

推论 IV　$\widetilde{G}$ 是弱完备的.

证明与 11.2 节中对于实数所给的证明完全类似. 设 $\{\widetilde{x}_1, \widetilde{x}_2, \cdots\}$ 是 $\widetilde{G}$ 中的元素的一个序列, 它满足 Cauchy 收敛准则:

$$\widetilde{x}_\mu^{-1}\widetilde{x}_\nu \in \widetilde{V}, \quad \text{对 } \mu \geqslant m \text{ 和 } \nu \geqslant m.$$

我们在 G 中选取 e 的一个可数邻域基 $\{U_1, U_2, \cdots\}$. 对每一 U_λ, 选取一个 V_λ 使得

$$V_\lambda^{-1}V_\lambda V_\lambda \subseteq U_\lambda.$$

此外, 我们可以取

$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots.$$

邻域 V_λ 决定 F 中邻域 $\overline{V}_\lambda$, 它又决定 $\widetilde{G}$ 中邻域 $\widetilde{V}_\lambda$. 由推论 III, 每一 $\widetilde{x}_\mu$ 都是 G 中元素的序列的极限. 所以对于 $\widetilde{x}_\mu$ 可以由 G 中选取一个 y_μ, 使得

$$\widetilde{x}_\mu^{-1}y_\mu \in \widetilde{V}_\mu.$$

我们证明, y_μ 构成一个基本序列. 有

$$y_\mu^{-1}y_\nu = (y_\mu^{-1}\widetilde{x}_\mu)(\widetilde{x}_\mu^{-1}\widetilde{x}_\nu)(\widetilde{x}_\nu^{-1}y_\nu) \in \widetilde{V}_\mu^{-1}(\widetilde{x}_\mu^{-1}\widetilde{x}_\nu)\widetilde{V}_\nu. \tag{20.7}$$

对于每一 λ, 存在 $m \geqslant \lambda$, 使得

$$\widetilde{x}_\mu^{-1}\widetilde{x}_\nu \in \widetilde{V}_\lambda, \quad \text{对于 } \mu \geqslant m, \nu \geqslant m.$$

由 (20.7) 得, 对于 $\mu \geqslant m \geqslant \lambda$ 及 $\nu \geqslant m \geqslant \lambda$ 有

$$y_\mu^{-1}y_\nu \in \widetilde{V}_\mu^{-1}\widetilde{V}_\lambda\widetilde{V}_\nu \subseteq \widetilde{V}_\lambda^{-1}\widetilde{V}_\lambda\widetilde{V}_\lambda \subseteq \widetilde{U}_\lambda,$$

即 $y_\mu^{-1}y_\nu \in U_\lambda$. 所以 y_μ 构成 G 中一个基本序列. 这个基本序列决定 $\widetilde{G}$ 中一个元素 $\widetilde{y}$, 并且由推论 III, 有极限 $\widetilde{y}$. $\widetilde{x}_\mu$ 也以 $\widetilde{y}$ 为极限, 因为我们有

$$\widetilde{y}^{-1}\widetilde{x}_\mu = (\widetilde{y}^{-1}y_\mu)(y_\mu^{-1}\widetilde{x}_\mu),$$

并且对于充分大的 μ, 等号右端的两个因子都在 e 的任意小的邻域内. 因此基本序列 $\{\widetilde{x}_\mu\}$ 在 $\widetilde{G}$ 中有极限, 从而群 $\widetilde{G}$ 是弱完备的.

对于不满足可数公理 (A_1) 的 (T_1) 群来说, 在适当的前题下, 也可以使它完备化. 不过, 此时要用所谓 Cauchy 滤网来代替基本序列, 引进"完备"概念的定义及完备扩张的构造. Bourbaki N (Eléments de Mathématique, Livre III, Chap. III: Groupes topologiques. *Actualités Scient.*, 916) 已经很好地这样做了. 下面将作深入探讨.

习题 20.14 若 G 满足公理 (T_1) 和 (A_1), 则 G 中每一完备子群 H 都在 G 中是闭的 (利用习题 20.8)

20.10　滤　网

设 M 是一个固定的集合. M 的子集记为 $A, B, \cdots$. 并用大写德文字母 $\mathfrak{F}, \mathfrak{G}, \cdots$ 记这些子集的族.

子集族 $\mathfrak{F}$ 如果具有下列性质, 就被称为滤网：

(F_1)：如果集合 A 包含 $\mathfrak{F}$ 里的一个集合, 则一定属于 $\mathfrak{F}$.

(F_2)：$\mathfrak{F}$ 内有限多个集合的交仍属于 $\mathfrak{F}$.

(F_3)：空集不属于 $\mathfrak{F}$.

从 (F_2) 可知, M 自己作为空的子集族的交也属于 $\mathfrak{F}$. 我们也可以用以下两个条件代替 F_2：

(F_2')：$\mathfrak{F}$ 内两个集合的交仍属于 $\mathfrak{F}$.

(F_2'')：M 属于 $\mathfrak{F}$.

例　拓扑空间 M 内点 p 的邻域构成一个滤网, 即点 p 的邻域滤网.

非空子集族 $\mathfrak{B}$ 如果具有下列性质, 就被称为滤网基：

B_1：$\mathfrak{B}$ 内两个集合的交一定包含 $\mathfrak{B}$ 的一个集合.

B_2：空集不属于 $\mathfrak{B}$.

如果这些性质被满足, 我们就可以构造一个滤网 $\mathfrak{F}$, 它由 M 内至少包含 $\mathfrak{B}$ 中一个集合的子集组成. 称这个滤网为 $\mathfrak{B}$ 生成的滤网, 称 $\mathfrak{B}$ 为这个滤网 $\mathfrak{F}$ 的基.

例　拓扑空间 M 内点 p 的基本邻域构成 p 的邻域滤网的基.

例　给定 M 的元素的序列

$$a_1 a_2 a_3 \cdots.$$

从中删去有限多个元素后, 剩下的元素可以构成一个集合 A. 这些集合 A 构成滤网基 $\mathfrak{B}$. 由 $\mathfrak{B}$ 生成的滤网是由 M 的包含此序列几乎所有的项的集合构成.

以后我们把 M 取成拓扑群 G. 设 V 是恒等元 e 的邻域. A 是一个集合, 如果它的元素之商 $x^{-1}y$ 总是在 V 内, 即

$$x^{-1}y \in V, \quad \text{因此 } y \in xV, \text{对任意的 } x, y \in A,$$

就称 A 与 V 同阶小.

如果对于 e 的任意邻域 V, 都有 $\mathfrak{B}$ 的集合 A, 使得 A 与 V 同阶小, 就称 $\mathfrak{B}$ 包含任意小集合.

包含任意小集合的滤网称为Cauchy 滤网.

包含任意小集合的滤网基 $\mathfrak{B}$ 称为 G 内的Cauchy 滤网基. 由 Cauchy 滤网基生成的滤网是 Cauchy 滤网.

若 $\mathfrak{B}$ 是一个滤网基, 使得 a 的每个邻域都包含 $\mathfrak{B}$ 的一个集合 A, 就称 $\mathfrak{B}$ 收敛到 a, 记为

$$\lim \mathfrak{B} = a.$$

在 T_1 群里极限 a 是唯一确定的.

在 20.9 节里把所有 Cauchy 序列都有极限的 T_1 群称为弱完备的. 不过这个概念只能适用于满足第一可数公理的群. 对于一般情形, 我们需要更强的概念. 因此把使得所有 Cauchy 滤网都在 G 内收敛的群称为强完备的.

这里定义的完备概念确实比以前定义的强: *强完备 T 群都是弱完备的.*

证 设 G 是强完备的, 并且 $\{x_\nu\}$ 是 G 内的基本序列. 根据 Cauchy 序列的定义, 从序列中删去有限多个项后得到的集合 A 是任意小的. 这些集合构成了 Cauchy 滤网基 $\mathfrak{B}$, $\mathfrak{B}$ 又生成 Cauchy 滤网 $\mathfrak{F}$. 这个滤网在 G 内有极限 a. 而 a 的每个邻域包含序列几乎所有的项 x_ν, 所以此序列在 G 内有极限 a.

根据 Bourbaki 的论述, 我们现在证明以下命题:

如果集合 D 在 T_1 群 G 内稠密, 而且 D 内的任意 Cauchy 滤网基在 G 内收敛到一个极限, 则 G 是强完备的.

证 设 $\mathfrak{F}$ 是 G 的 Cauchy 滤网, 我们要证明 $\mathfrak{F}$ 收敛.

对于 e 的每个邻域 V 以及滤网 $\mathfrak{F}$ 的每个集合 A, 作出乘积 AV. 这些集合构成滤网基 $\mathfrak{B}$, 这是因为对于这样的集合 AV 和 $A'V'$, 集合

$$(A \cap A')(V \cap V')$$

包含在 AV 和 $A'V'$ 的交集里. 现在证明 $\mathfrak{B}$ 是 Cauchy 滤网基.

设 U 是 e 的邻域, V 是使得 $V^{-1}VV$ 包含在 U 内的邻域. 我们选取与 V 同阶小的 A. 这样对于 AV 的任意两个元素 $av, a'v'$ 有

$$(av)^{-1}a'v' = v^{-1}(a^{-1}a')v' \in V^{-1}VV \subseteq U,$$

从而 AV 是与 U 同阶小的. $\mathfrak{B}$ 是 Cauchy 滤网基.

由于 A 包含至少一个元素 a, 而且在 a 的任意邻域 aV 里至少有 D 的一个点, 所以乘积集 AV 与 D 的交集非空. 因此交集 $AV \cap D$ 构成 D 的 Cauchy 滤网基. 根据假设, 它在 G 内有一个极限 b. 在 b 的每个邻域里含有一个集合 AV, 从而也含有子集 $Ae = A$. 所以 $\mathfrak{F}$ 收敛到 b, 证毕.

习题 20.15 如果滤网 $\mathfrak{F}$ 收敛到 a, 则 $\mathfrak{F}$ 是 Cauchy 滤网.

习题 20.16 如果滤网基 $\mathfrak{B}$ 收敛到 a, 则由 $\mathfrak{B}$ 生成的滤网 $\mathfrak{F}$ 也收敛到 a. 反过来也对.

习题 20.17 如果一个 T 群是弱完备的, 并且满足第一可数公理, 那么它也是强完备的.

提示: 设 $V_1, V_2, \cdots$ 是 e 的可数邻域基, 设 $\mathfrak{F}$ 是 Cauchy 滤网. 对于每个 n, 在滤网里有一个与 V_n 同阶小的集合 A_n. 作交集

$$D_n = A_1 \cap A_2 \cap \cdots \cap A_n,$$

并在 D_n 内选取 x_n, 则 $\{x_n\}$ 是基本序列, 它的极限也是滤网 $\mathfrak{F}$ 的极限.

20.11 用 Cauchy 滤网作群的完备化

作为强完备化的准备, 我们先证明类似于 20.9 节的一个引理, 其证明方法也是类似的.

设 $\mathfrak{F}$ 是 Cauchy 滤网. 则对 e 的任意邻域 U, 存在邻域 V 以及 $\mathfrak{F}$ 里的集合 A, 使得

$$x^{-1}Vx \subseteq U, \quad \text{对所有的 } x \in A.$$

证 选取 W 使得 $WWW \subseteq U$, 选取 A 使得

$$x^{-1}y \in W, \quad \text{对 } x, y \in A.$$

取定 y, 则当 $x \in A$ 时有 $x^{-1}y$ 和 $y^{-1}x$ 属于 W. 根据 20.6 节的 (E_4), 可以在 yWy^{-1} 内选取一个 V. 于是对所有的 $x \in A$ 有 $x^{-1}Vx \subseteq (x^{-1}y)W(y^{-1}x) \subseteq WWW \subseteq U$.

设 $\mathfrak{F}$ 和 $\mathfrak{G}$ 是两个滤网, 我们把由乘积 AB (其中 $A \in \mathfrak{F}, B \in \mathfrak{G}$) 生成的滤网 $\mathfrak{F}\mathfrak{G}$ 称为它们的积. 积满足结合律:

$$\mathfrak{F} \cdot \mathfrak{G}\mathfrak{H} = \mathfrak{F}\mathfrak{G} \cdot \mathfrak{H}. \tag{20.8}$$

这是因为 (20.8) 式的两边都等于由乘积 ABC (其中 $A \in \mathfrak{F}, B \in \mathfrak{G}, C \in \mathfrak{H}$) 生成的滤网.

I. *若 $\mathfrak{F}$ 和 $\mathfrak{G}$ 是 Cauchy 滤网, 则 $\mathfrak{F}\mathfrak{G}$ 也是 Cauchy 滤网.*

证 我们有

$$(xy)^{-1}x'y' = y^{-1}(x^{-1}x')y(y^{-1}y'). \tag{20.9}$$

若 x 和 x' 包含在 $\mathfrak{F}$ 的适当选取的集合 A 内, y 和 y' 包含在 $\mathfrak{G}$ 的适当选取的集合 B 内, 则 $x^{-1}x'$ 和 $y^{-1}y'$ 落在 e 的任意小邻域内. 根据引理, $y^{-1}(x^{-1}x')y$ 落在一个任意小邻域 U 内. 所以乘积 (20.9) 落在 e 的一个任意小邻域内, 证毕.

II. *若 $\mathfrak{F}$ 是 Cauchy 滤网, $\mathfrak{G}$ 收敛到 e, 则 $\mathfrak{F}^{-1}\mathfrak{G}\mathfrak{F}$ 收敛到 e.*

证 若 x 和 x' 包含在滤网 $\mathfrak{F}$ 的集合 A 内, y 包含在滤网 $\mathfrak{G}$ 的集合 B 内, 则在 e 一个任意小的邻域 V 内适当选取 B 可以使得

$$x^{-1}yx' = x^{-1}yx \cdot x^{-1}x'$$

$$\subseteq x^{-1}Vx \cdot U. \tag{20.10}$$

根据引理, 通过适当选取 V 和 A, 可使 $x^{-1}Vx$ 包含在 e 一个任意小邻域 U 内. 所以乘积 (20.10) 落在 $U \cdot U$ 内, 从而在 e 的任意小邻域内.

习题 20.18 所有包含 e 的集合 A 构成一个 Cauchy 滤网 $\mathfrak{E}$. 这个滤网是滤网乘法的单位元:

$$\mathfrak{E}\mathfrak{F} = \mathfrak{F}\mathfrak{E} = \mathfrak{F}, \quad \text{对所有的 } \mathfrak{F}.$$

像 20.9 节所做的那样, 我们现在要引入*群完备化公理*, 它是 (TG_3) 的强版本:

(GC)*如果 $\mathfrak{F}$ 是 Cauchy 滤网, 则 $\mathfrak{F}^{-1}$ 也是 Cauchy 滤网.*

这意味着如果乘积 $x^{-1}y$ (其中 x 和 y 在 $A \in \mathfrak{F}$ 内) 包含在 e 的任意小邻域内, 则乘积 yx^{-1} 也包含在 e 的任意小邻域内. 在 Abel 群里这是平凡的.

Cauchy 滤网关于乘法构成*半群*, 也就是说满足 2.1 节的前 3 条群公理. 公理 4 一般不满足. 每个 Cauchy 滤网 $\mathfrak{F}$ 确实有一个逆 Cauchy 滤网 $\mathfrak{F}^{-1}$, 但是在大多数情况下乘积 $\mathfrak{F}^{-1}\mathfrak{F}$ 不等于 $\mathfrak{E}$.

用 $\hat{G}$ 表示 G 的 Cauchy 滤网的半群. 我们可以通过定义单位元 $\mathfrak{E}$ 的基本邻域 $\hat{U}$ 使得 $\hat{G}$ 成为一个拓扑空间: 对 e 在 G 里的邻域 U, 定义基本邻域 $\hat{U}$ 如下: $\hat{U}$ 由所有至少包含一个集合 $A \subseteq U$ 的滤网 $\mathfrak{F}$ 构成.

这样定义的基本邻域 $\hat{U}$ 满足 20.6 节的条件 (E_1)~(E_5). (E_1) ~(E_3) 以及 (E_5) 是显然的, 而证明 (E_4) 需要用到前面的引理.

习题 20.19 证明 (E_4).

习题 20.20 收敛到 e 的滤网就是那些位于所有邻域 $\hat{U}$ 里的滤网.

如同 20.6 节, 我们可以利用邻域 $\hat{U}$ 来构成平移邻域 $\mathfrak{F}\hat{U}$. 这样就使 $\hat{U}$ 成为拓扑空间. 在这个拓扑的意义下, 乘积 $\mathfrak{F}\mathfrak{G}$ 和求逆 $\mathfrak{F}^{-1}$ 是连续的. 所以 $\hat{G}$ 成为*拓扑半群*. 但分离公理 (T_1) 一般不满足 (参见习题 20.20).

收敛到 e 的滤网构成 $\hat{G}$ 里的子半群 $\hat{N}$. 根据 II, $\hat{N}$ 是下述意义下的正规子半群:

$$\mathfrak{F}^{-1}\hat{N}\mathfrak{F} \subseteq \hat{N}, \quad \text{对所有的 } \mathfrak{F}.$$

由于 $\hat{G}$ 和 $\hat{N}$ 的上述性质, 以及以下显然的性质:

$$\mathfrak{F}^{-1}\mathfrak{F} \in \hat{N},$$

使得我们可以构造商群

$$\hat{G}/\hat{N} = \tilde{G}.$$

注意在 2.5 节构造商群时并不需要性质 $a^{-1}a = e$ (这里是 $\mathfrak{F}^{-1}\mathfrak{F} = \mathfrak{E}$), 而是只需 $\mathfrak{F}^{-1}\mathfrak{F} \in \hat{N}$ 就够了. 因此上述商群确实是一个群, 其中每个元素都有一个真正的逆.

如同 20.7 节, 我们看到商群 $\hat{G}/\hat{N}$ 是一个 T 群. 存在从 $\hat{G}$ 到 $\hat{G}/\hat{N}=\tilde{G}$ 上的连续同态.

根据习题 20.20, $\hat{N}$ 正是由那些不能与群 $\hat{G}$ 的恒等元 $\mathfrak{E}$ 分离的滤网 $\mathfrak{F}$ 构成. 根据 20.6 节, $\hat{N}$ 闭, 因此 $\tilde{G}=\hat{G}/\hat{N}$ 是 T_1 群.

每个元素 $x\in G$ 可以定义一个滤网 $\mathfrak{F}_x$, 它由所有含 x 的集合 A 组成.

这个滤网包含集合 $\{x\}$, 因此是 Cauchy 滤网. 所以每个 $x\in G$ 可以对应 $\hat{G}$ 的一个 $\hat{x}=\mathfrak{F}_x$. 这个对应 $x\to\hat{x}$ 是连续的, 并且把乘积映到乘积. 同态 $\hat{G}\to\tilde{G}$ 把元素 $\hat{x}$ 映到象 $\tilde{x}$. 因而有连续同态的链

$$x\to\hat{x}\to\tilde{x}. \tag{20.11}$$

如果元素 x 和 y 在 G 内不可分, 则它们在 $\tilde{G}$ 内有同一个象 $\tilde{x}$, 反之亦对.

以后假设 G 是 T_1 群. 因此其中任意两个不同的元 x 和 y 是可分的, 从而映射 $x\to\tilde{x}$ 是 1–1 的. 所以, G 嵌入 $\tilde{G}$.

现设 $\mathfrak{B}$ 是 G 里的 Cauchy 滤网基. 由于 G 嵌入 $\tilde{G}$, 我们可以把 $\mathfrak{B}$ 看成 $\tilde{G}$ 内的滤网基. 另一方面, $\mathfrak{B}$ 生成 G 内的 Cauchy 滤网 $\mathfrak{F}$, 这个滤网在同态 $\hat{G}\to\tilde{G}$ 下对应 $\tilde{G}$ 的元 $\tilde{a}$. 我们现在证明以下断言：

III. 滤网基 $\mathfrak{B}$ 收敛到 $\tilde{a}$.

证　根据 Cauchy 滤网基的定义, 对于 e 的每个邻域 U, 存在 $\mathfrak{B}$ 内的集合 A, 使得

$$y^{-1}x\in U,\quad 对所有的\ x,y\in A.$$

这也可以写成

$$A^{-1}x\subseteq U,\quad 对所有的\ x\in A.$$

集合 A^{-1} 属于滤网 $\mathfrak{F}^{-1}$, 集合 $\{x\}$ 属于滤网 $\hat{x}$, 所以乘积 $\mathfrak{F}^{-1}\hat{x}$ 包含在集合 $A^{-1}\{x\}\subseteq U$ 内. 由 $\hat{G}$ 内邻域 $\hat{U}$ 的定义, 这意味着

$$\mathfrak{F}^{-1}\hat{x}\in\hat{U},\quad 对所有的\ x\in A.$$

通过连续同态从 $\hat{G}$ 转移到 $\tilde{G}$, 可得

$$\tilde{a}^{-1}\tilde{x}\in\tilde{U},$$

从而

$$\tilde{x}\in\tilde{a}\tilde{U}.$$

我们已经把 $\tilde{x}$ 等同于 x, 所以有

$$x\in\tilde{a}\tilde{U},\quad 对所有的\ x\in A.$$

即

$$A \subseteq \tilde{a}\tilde{U}.$$

因此, 在滤网基 $\mathfrak{B}$ 里存在一个集合 A, 它包含在 $\tilde{a}$ 的任意小邻域 $\tilde{a}\tilde{U}$ 内, 也就是 $\mathfrak{B}$ 收敛到 $\tilde{a}$. III 获证.

由于在 $\tilde{a}$ 的每个邻域里都存在非空集合 A, 因此总有 G 的点落在 $\tilde{a}$ 的任一邻域里. 这说明 G 在 $\tilde{G}$ 内稠密.

从这个结果, 加上 III 以及 20.10 节最后的定理, 我们得到

IV. $\tilde{G}$ *是强完备的*.

习题 20.21 如果第一可数公理在 G 内成立, 则它在 $\tilde{G}$ 内也成立. 此时 $\tilde{G}$ 的每个元素都是 G 内一个序列 $\{x_\nu\}$ 的极限. 而且从 20.9 节中 G 的弱完备性可以导出与 20.11 节中的强完备性同样的结果.

20.12 拓扑向量空间

一个交换的加法 T 群叫做一个 T 模M. 根据 20.6 节, M 里的拓扑是通过满足 20.6 节末尾的条件 (1)~(3) 的零元的邻域系 U 定义的.

20.9 节和 20.11 节的概念在加法 T 群里仍然有效. 基本序列 $\{x_\nu\}$ 是这样刻画的: 对于零元的任一邻域 V, 只要 μ 和 ν 充分大, 差 $x_\mu - x_\nu$ 就在 V 内. 如果集合 A 的任意元素 x, y 之差 $y - x$ 总在 V 内, 就称 A *是与 V 同阶小的*. 包含任意小集合的滤网称为 Cauchy 滤网. 如果 M 里的任意 Cauchy 滤网都收敛, 就称模 M 是*强完备的*, 或简称完备的.

因为根据 20.11 节, 对于交换群不需要完备公理, 所以每一 T_1 模 M 都可以嵌入一个完备的 T_1 模 $\tilde{M}$ 中.

现在设模 M 带有一个*算子集* Ω, 并且每个算子 γ 都具有性质

$$\gamma(a+b) = \gamma a + \gamma b. \tag{20.12}$$

我们假定 γx 是 x 的连续函数, 也就是说, 对于每个 U 存在一个 V 满足

$$\gamma V \subseteq U.$$

如果滤网 $\mathfrak{F}$ 含有任意小的集合, 则 $\gamma\mathfrak{F}$ 也含有任意小集合 γA, 即 $\gamma\mathfrak{F}$ 仍是 Cauchy 滤网. 因此 20.11 节的完备化理论可以立即推广到带算子的 T_1 模, 其完备模 $\tilde{M}$ 有相同的算子集 Ω.

有时候我们有目的地把 γa 改写成 $a\gamma$. 这时称 Ω 为*右算子集*而 M 称为 Ω*右模*. 于是代替 (20.12) 有

$$(a+b)\gamma = a\gamma + b\gamma. \tag{20.13}$$

如果 Ω 是一个环, 那么除了 (20.13) 以外, 还要求下列运算规则:

$$a(\beta+\gamma)=a\beta+a\gamma. \tag{20.14}$$

$$a(\beta\gamma)=(a\beta)\gamma. \tag{20.15}$$

过渡到完备模 $\tilde{M}$ 的时候, 这些关系仍然成立.

若 Ω 是一个 T 环, 则要求乘积 $x\gamma$ 是 x 与 γ 的连续函数. 这些性质也转移到基本序列上, 从而 $\tilde{M}$ 是一个完备的 Ω 右模.

若 Ω 是一个体, 除了上面所列举的运算规则外, 还有

$$a\cdot 1=a, \tag{20.16}$$

其中 1 是 Ω 的单位元, 那么称 M 为 Ω 上的一个向量空间. 若 Ω 是一个 T 体, 那么也要求乘积 $x\gamma$ 是 x 和 γ 的连续函数.

T 体 Ω 上的拓扑向量空间的一个简单例子是典范的 n 维向量空间 Ω^n, 它由所有 Ω 中 n 个元素的有序元素列 $(\beta_1,\cdots,\beta_n)$ 组成. 向量与 Ω 中元素的乘法定义为

$$(\beta_1,\cdots,\beta_n)\gamma=(\beta_1\gamma,\cdots,\beta_n\gamma).$$

零向量的一个基邻域 U' 由一切这样的向量 $(\beta_1,\cdots,\beta_n)$ 所组成, 其中每一坐标 $\beta_1,\cdots,\beta_n$ 都在 Ω 的零元的某一基邻域 U 内. 邻域公理以及加法和乘法的连续性都成立.

若 Ω 是完备的, 则 Ω^n 也是完备的.

证　向量 $(\beta_1,\cdots,\beta_n)$ 的集合 A 与 U' 同阶小的充分必要条件是对每个 i, β_i 的集合与 U' 同阶小. 我们把 β_i 的集合称为集合 A 的 i 分量, 记为 A_i. 如果给出了集合 A 的 Cauchy 滤网 $\mathfrak{F}$, 则对每个 i, A_i 构成 Ω 里的 Cauchy 滤网. 若 Ω 是完备的, 则所有这些 Cauchy 滤网在 Ω 里有极限 γ_i. 这样对每个 U, 存在 1 分量在 γ_1+U 里的集合 $A^{(1)}$, 2 分量在 γ_2+U 里的集合 $A^{(2)}$, 直至 $A^{(n)}$. 交集

$$A=A^{(1)}\cap A^{(2)}\cap\cdots\cap A^{(n)}$$

在 $(\gamma_1,\cdots,\gamma_n)+U'$ 内. 因此滤网 $\mathfrak{F}$ 收敛于极限 $(\gamma_1,\cdots,\gamma_n)$.

20.13　环的完备化

T_1 环 R 是一个加法 T_1 群, 并且可以扩张成强完备群

$$\tilde{R}=\hat{R}/\hat{N},$$

这里的 $\hat{R}$ 是 Cauchy 滤网的加法群, $\hat{N}$ 是由以零为极限的滤网构成的正规子群.

我们要定义 $\hat{R}$ 里的乘法, 使得 $\hat{R}$ 成为环, $\hat{N}$ 成为环里的双边理想, 从而 $\tilde{R}=\hat{R}/\hat{N}$ 成为完备 T 环.

我们仍用 $U, V, W, \cdots$ 记零元的邻域. 首先证明以下引理.

引理 *如果 $\mathfrak{F}$ 是 Cauchy 滤网, 则对每个 U, 存在一个 W 以及 $\mathfrak{F}$ 里的集合 A, 使得*

$$AW \subseteq U \quad \text{以及} WA \subseteq U.$$

证 存在 U', 使得

$$U'+U' \subseteq U.$$

存在 V, 使得

$$V \cdot V \subseteq U'.$$

存在 $\mathfrak{F}$, 里的集合 A 满足

$$x-y \in V, \quad \text{对所有的 } x, y \in A.$$

如果取定 $y \in A$, 则存在 $W \subseteq V$, 使得

$$yW \subseteq U' \quad \text{以及} Wy \subseteq U'.$$

则对每个 $x \in A$ 以及 $z \in W$,

$$xz=(x-y)z+yz \in VV+yW \subseteq U'+U' \subseteq U,$$

从而 $AW \subseteq U$. 同理可证 $WA \subseteq U$.

从这个引理可得以下推论.

I. *若 $\mathfrak{F}$ 和 $\mathfrak{G}$ 是 Cauchy 滤网, 则 $\mathfrak{F}\mathfrak{G}$ 也是 Cauchy 滤网.*

证 我们有

$$xy-x'y'=x(y-y')+(x-x')y'. \tag{20.17}$$

对给定的 U, 可选取 V, 使得

$$V+V \subseteq U.$$

由引理, 存在 $\mathfrak{F}$ 里的 A, $\mathfrak{G}$ 里的 B, 以及一个 W, 使得

$$WB \subseteq V \quad \text{以及} AW \subseteq V.$$

若 xy 和 $x'y'$ 是 AB 的元 $(x, x' \in A,\ y, y' \in B)$, 则由 (20.17) 可得

$$xy-x'y' \in V+V \subseteq U.$$

因此 $\mathfrak{F}\mathfrak{G}$ 是 Cauchy 滤网.

II. 如果 $\mathfrak{F}$ 是 Cauchy 滤网, $\mathfrak{G}$ 收敛到零, 则 $\mathfrak{F}\mathfrak{G}$ 和 $\mathfrak{G}\mathfrak{F}$ 也收敛到零.

II 的证明可从引理直接得出.

由 I, Cauchy 滤网构成环 $\hat{R}$. 由 II, 收敛到零的滤网构成这个环的双边理想 $\hat{N}$. 所以商模

$$\tilde{R} = \hat{R}/\hat{N}$$

不仅是完备 T 模, 也是一个环.

我们现在要证明 $\hat{R}$ 内乘法的连续性.

III. 如果 $\mathfrak{F}$ 和 $\mathfrak{G}$ 是 Cauchy 滤网, 且若 $\hat{U}$ 是 $\hat{R}$ 内零元的基本邻域 (见 20.11 节定义), 则存在基本邻域 $\hat{V}$ 和 $\hat{W}$, 使得

$$(\mathfrak{F} + \hat{V})(\mathfrak{G} + \hat{W}) \subseteq \mathfrak{F}\mathfrak{G} + \hat{U}. \tag{20.18}$$

证 对任意的 $x, y, v, w \in R$,

$$(x+v)(y+w) = xy + xw + vy + vw. \tag{20.19}$$

现设给定了 R 内零元的邻域 U, 我们选取 U' 使得 $U' + U' + U' \subseteq U$. 然后根据引理选取 $\mathfrak{F}$ 内的 A, $\mathfrak{G}$ 内的 B, 以及邻域 V', W', 使得

$$AV' \subseteq U' \quad \text{以及} W'B \subseteq U'.$$

最后取 $V \subseteq V'$, $W \subseteq W'$ 使得 $VW \subseteq U'$. 根据 (20.19) 可知, 对 $x \in A$, $y \in B$, $v \in V$ 以及 $w \in W$, 有

$$(x+v)(y+w) \in xy + U' + U' + U' \subseteq xy + U,$$

所以

$$(A+V)(B+W) \subseteq AB + U.$$

这样就证明了 III.

因此 $\hat{R}$ 是 T 环, 故 $\tilde{R}$ 也是 T 环, 又因 $\tilde{R}$ 满足第一分离公理, 它还是 T_1 环.

由 20.11 节知 $\tilde{R}$ 是完备的. 因此每个 T_1 环可被嵌入到一个完备 T_1 环.

20.14 体的完备化

设 S 是满足第一分离公理的 T 体. 由 20.13 节, S 可被嵌入到一个完备 T 环 $\tilde{S} = \hat{S}/\hat{N}$. 由于 $\tilde{S}$ 的元素 $w \neq 0$ 的逆元不一定存在, 即使存在也不一定连续依赖于 w, 因此 $\tilde{S}$ 不一定是 T 体.

下述体的完备化公理是保证 S 可被嵌入一个完备 T 体的充分必要条件.

(SF) 若 $\mathfrak{F}$ 是 S 内不收敛到零的 Cauchy 滤网, 则 $\mathfrak{F}^{-1}$ 是 Cauchy 滤网的基.

我们先证明 (SF) 是使 S 可嵌入完备 T 体的必要条件. S 里的 Cauchy 滤网 $\mathfrak{F}$ 在此嵌入下给出了一个 Cauchy 滤网的基, 这个滤网在 $\tilde{S}$ 内有极限 $a \neq 0$. 由于映射 $x \to x^{-1}$ 是连续的, 逆滤网基 $\mathfrak{F}^{-1}$ 收敛到 a^{-1}. 所以 $\mathfrak{F}^{-1}$ 是 Cauchy 滤网的基.

现在假设 (SF) 被满足, 我们要证明 S 是完备 T 体.

我们首先证明前面的公理 (TS)(20.8 节) 可从 (SF) 导出. 设 U 是 S 内零元的邻域. 我们要证明存在一个邻域 V 使得

$$(1+V)^{-1} \subseteq 1+U.$$

单位元的邻域 $1+V$ 构成一个 Cauchy 滤网 $\mathfrak{F}$, 它收敛到 1, 因此不收敛到 0. 根据 (SF), $\mathfrak{F}^{-1} = \mathfrak{B}$ 是 Cauchy 滤网的基. $\mathfrak{B}$ 内的集合是

$$A = (1+V)^{-1},$$

当然要把 $1+V$ 中的 0 略去. 对于 $1+V$ 里的每个 $y \neq 0$ 有

$$1 - y^{-1} = y^{-1}(y-1) \in AV. \tag{20.20}$$

根据 20.13 节的引理, 对于每个 U, 存在 W 以及 $\mathfrak{B}$ 里的 A', 使得

$$A'W \subseteq -U.$$

这个 A' 具有 $(1+V')^{-1}$ 的形式. 我们在交集 $V' \cap W$ 里选取 V. 则有 $A \subseteq A'$ 与 $V \subseteq W$, 于是

$$AV \subseteq A'W \subseteq -U,$$

$$1 - y^{-1} \in -U,$$

$$y^{-1} - 1 \in U,$$

$$y^{-1} \in 1+U.$$

这对 $1+V$ 里的所有 $y \neq 0$ 成立, 因此可得我们欲证的

$$(1+V)^{-1} \subseteq 1+U. \tag{20.21}$$

我们现在可证 $\tilde{S}$ 里的任意 $a \neq 0$ 有一个逆. 元素 a 是 S 中一个 Cauchy 滤网 $\mathfrak{F}$ 的极限. 由 (SF), $\mathfrak{F}^{-1}$ 是一个 Cauchy 滤网的基, 这个滤网在 $\tilde{S}$ 里有极限 b. 乘积 $\mathfrak{F}^{-1}\mathfrak{F}$ 一方面有极限 ba, 另一方面又有极限 1, 因此 $ba = 1$.

为证 $\tilde{S}$ 是体, 根据 20.8 节, 只需证明对于零元的每个基本邻域 $\tilde{U}$, 存在零元的基本邻域 $\tilde{V}$, 使得

$$(1+\tilde{V})^{-1} \subseteq 1+\tilde{U}.$$

基本邻域 $\tilde{U}$ 和 $\tilde{V}$ 是从 $\hat{S}$ 的基本邻域 $\hat{U}$ 和 $\hat{V}$ 通过同态 $\hat{S} \to \tilde{S}$ 得到的. 因此只需证明

$$(1+\hat{V})^{-1} \subseteq 1+\hat{U}.$$

不过只要回忆一下 $\hat{U}, \hat{V}$ 与 U, V 的关系, 就立即能从 (20.21) 导出要证的包含关系.

现在我们可以归纳成一下结论:

*如果 (SF) 满足, 那么 $\tilde{S}$ 是 T 体. 因此 (SF) 是使 S 能嵌入完备 T 体的充分必要条件.*①

---

① 对拓扑体的进一步研究可参看:

Kaplanski I. Topological Methods in Valuation Theory. *Duke Math. J.*, 1947, 14:527.

Kowalsky H J and Dürbaum H. Arithmetische Kennzeichnung von Körpertopologien. *J. Reine u. Angew. Math.*, 1953, 191: 135.

Kowalsky H J. Zur Topologischen Kennzeichnung von Körpern. *Math. Nachr.*, 1953, 9: 261.

Pontrjagin L S. *Topologische Gruppen.* Teubner, Leipzig, 1957.

索　　引

六　　画

七　画

八　画

九 画

十　画

十 一 画

十 二 画

十 三 画

十 四 画

十 五 画

十 六 画

其 他